Benutzerhandbuch

Novell® PlateSpin Forge®

3.1

Oktober 2011

www.novell.com



Rechtliche Hinweise

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
USA.
www.novell.com

Online-Dokumentation: Die neueste Online-Dokumentation für dieses und andere Novell-Produkte finden Sie auf der Dokumentations-Webseite (http://www.novell.com/documentation) von Novell.

Novell-Marken

Hinweise zu Novell-Marken finden Sie in der Novell Trademark and Service Mark-Liste (http://www.novell.com/company/legal/trademarks/tmlist.html).

Materialien von Drittanbietern

Die Rechte für alle Marken von Drittanbietern liegen bei den jeweiligen Eigentümern.

Inhalt

Informationen zu diesem Handbuch

Dieses Handbuch enthält Informationen zur Verwendung von PlateSpin Forge.

Zielgruppe

Dieses Handbuch ist für IT-Mitarbeiter wie beispielsweise Rechenzentrumsadministratoren und -operatoren vorgesehen, die PlateSpin Forge in Workload-Schutzprojekten verwenden.

Rückmeldungen

Wir freuen uns über Ihre Hinweise, Anregungen und Vorschläge zu diesem Handbuch und den anderen Teilen der Dokumentation zu diesem Produkt. Bitte verwenden Sie die Funktion für Benutzerkommentare im unteren Bereich jeder Seite der Online-Dokumentation oder senden Sie uns Ihre Kommentare über die Novell Documentation Feedback-Website (http://www.novell.com/documentation/feedback.html).

Weitere Dokumentation

Dieses Handbuch ist Bestandteil der PlateSpin Forge-Dokumentation.

Eine vollständige Liste der Publikationen, die diese Version unterstützen, finden Sie auf der Website mit der Online-Dokumentation für PlateSpin Forge 3 (http://www.novell.com/documentation/platespin_forge_3).

Aktualisierungen der Dokumentation

Die neueste Version dieses Handbuchs finden Sie auf der Online-Dokumentations-Website zu PlateSpin Protect 10 (http://www.novell.com/documentation/platespin_protect_10):

Zusätzliche Ressourcen

Wir empfehlen Ihnen, die folgenden zusätzlichen Ressourcen im Web zu nutzen:

- Novell User Forum (http://forums.novell.com): eine webbasierte Community mit verschiedenen Diskussionsthemen.
- Novell Knowledgebase (http://www.novell.com/support): eine Sammlung ausführlicher technischer Artikel.

Technischer Support

- Telefon (Nordamerika): +1-877-528-3774 (1 87 PlateSpin)
- Telefon (international): +1-416-203-4799
- Email: support@platespin.com

Sie können auch die Website für den technischen Support von PlateSpin (http://www.platespin.com/support) besuchen.

1 Produktübersicht

1.1 Informationen zu PlateSpin Forge

Bei PlateSpin Forge handelt es sich um eine konsolidierte Hardware-Appliance zur Wiederherstellung, die mithilfe integrierter Virtualisierungstechnologie sowohl physische als auch virtuelle Workloads (Betriebssysteme, Middleware und Daten) schützt. Kommt es zu einer Katastrophe oder zum Ausfall eines Produktionsservers, werden Workloads von der PlateSpin Forge-Recovery-Umgebung schnell aufgefangen und bis zur Wiederherstellung der Produktionsumgebung völlig normal ausgeführt.

PlateSpin Forge bietet folgende Vorteile:

- Gleichzeitiger Schutz mehrerer Workloads (10 bis 25, abhängig vom Modell)
- Testen des Failover-Workloads ohne Ihre Produktionsumgebung zu beeinträchtigen
- Schnelle Wiederherstellung von Workloads nach einem Fehler
- Unterstützung externer Speicherlösungen, z. B. SANs

Mit seinem internen Speicher verfügt Forge über eine Gesamtspeicherkapazität von 3.5 Terabyte. Allerdings lässt sich die Kapazität durch Verwendung von externen Speicherkonfigurationen, wie iSCSI- oder Fibre-Channel-Karten, nahezu unbegrenzt erweitern.

1.2 Unterstützte Konfigurationen

1.2.1 Unterstützte Workloads

PlateSpin Forge unterstützt sowohl Windows- als auch Linux-Workloads.

Tabelle 1-1 *Unterstützte Windows-Workloads*

Betriebssystem	Anmerkungen
Windows 7	Windows 7 Home Edition wird nicht unterstützt
Windows Server 2008 R2	Einschließlich Domänencontroller- und Small Business Server-Editionen
Windows Server 2008	Einschließlich Domänencontroller- und Small Business Server-Editionen
Windows Vista	Business-, Enterprise- und Ultimate-Editionen; SP1 und höher

Betriebssystem	Anmerkungen
Windows Server 2003	Einschließlich Domänencontroller- und Small Business Server-Editionen
Windows XP Professional	
Windows Server 2000	
Windows-Cluster	

Unterstützte internationale Versionen (Windows): Französisch, Deutsch, Japanisch, Chinesisch (traditionell) und Chinesisch (vereinfacht)

Tabelle 1-2 *Unterstützte Linux-Workloads*

Betriebssystem
Open Enterprise Server 2, SP2 und SP3
Oracle Enterprise Linux (OEL) 5.3, 5.4
SUSE Linux Enterprise Server (SLES) 9, 10, 11
Red Hat Enterprise Linux (RHEL) 4, 5

Unterstützte internationale Versionen (Linux): Alle internationalen Versionen dieser Linux-Systeme werden unterstützt.

1.3 Sicherheit und Datenschutz

PlateSpin Forge stellt Ihnen eine Reihe von Funktionen zur Verfügung, mit denen Sie Ihre Daten schützen und die Sicherheit Ihres Systems erhöhen können.

- Abschnitt 1.3.1, „Sicherheit der Workload-Daten bei der Übertragung“, auf Seite 12
- Abschnitt 1.3.2, „Sicherheit der Client-Server-Kommunikation“, auf Seite 13
- Abschnitt 1.3.3, „Sicherheit von Berechtigungsnachweisen“, auf Seite 13
- Abschnitt 1.3.4, „Benutzerautorisierung und -authentifizierung“, auf Seite 13

1.3.1 Sicherheit der Workload-Daten bei der Übertragung

Sie können den Workload-Schutz so konfigurieren, dass die Daten verschlüsselt werden, um die Übertragung Ihrer Workload-Daten sicherer zu machen. Wenn die Verschlüsselung aktiviert ist, werden über das Netzwerk reproduzierte Daten unter Verwendung von AES (Advanced Encryption Standard) verschlüsselt.

Sie können die Verschlüsselung für jeden Workload-Schutz über die Parameter in den Workload-Schutz-Details aktivieren oder deaktivieren. Weitere Informationen hierzu finden Sie in „Workload-Schutz-Details“ auf Seite 62.

1.3.2 Sicherheit der Client-Server-Kommunikation

Die Datenübertragung zwischen dem PlateSpin Forge-Server und dem PlateSpin Forge Web-Client kann entweder über HTTP (Standard) oder HTTPS (Hypertext Transfer Protocol Secure) erfolgen.

Um die Datenübertragung zwischen dem Client und dem Server abzusichern, müssen Sie SSL auf Ihrer Forge-VM aktivieren, die Serverkonfiguration entsprechend ändern (siehe „Parameter für das Aktivieren der SSL-Kommunikation“ auf Seite 31) und für die Angabe der Server-URL HTTPS verwenden.

1.3.3 Sicherheit von Berechtigungsnachweisen

Der Berechtigungsnachweis, den Sie für den Zugriff auf verschiedene Systeme (z. B. Workloads und Failback-Ziele) verwenden, wird in der PlateSpin Forge-Datenbank gespeichert und unterliegt daher denselben Sicherheitsmechanismen, die Sie für den Forge-VM implementiert haben.

Darüber hinaus sind Berechtigungsnachweise in der Diagnose enthalten, die für berechtigte Benutzer zugänglich ist. Sie sollten sicherstellen, dass Workload-Schutz-Projekte von befugten Mitarbeitern bearbeitet werden.

1.3.4 Benutzerautorisierung und -authentifizierung

PlateSpin Forge bietet einen umfassenden und sicheren Benutzerautorisierungs- und -authentifizierungsmechanismus, der auf Benutzerrollen basiert und den Anwendungszugriff sowie die Aktionen steuert, die Benutzer ausführen können. Weitere Informationen hierzu finden Sie in Abschnitt 2.2, „Einrichten der Benutzerautorisierung und -authentifizierung“, auf Seite 18.

1.4 Leistung

1.4.1 Allgemeines zu Produktleistungsmerkmalen

Die Leistungsmerkmale Ihres PlateSpin Forge-Produkts sind von einer Reihe von Faktoren abhängig, darunter:

- Hardware- und Softwareprofile Ihrer Ursprungs-Workloads
- Eigenschaften Ihrer Netzwerkbandbreite, -konfiguration und -bedingungen
- Die Anzahl der geschützten Workloads
- Die Anzahl der Volumes unter Schutz
- Die Größe der Volumes unter Schutz
- Dateidichte (Anzahl der Dateien pro Kapazitätseinheit) auf den Volumes des Ursprungs-Workloads
- Ursprungs-E/A-Ebenen (die Auslastung Ihrer Workloads)
- Die Anzahl der gleichzeitigen Reproduktionen

- Ob die Datenverschlüsselung aktiviert oder deaktiviert ist
- Ob die Datenkomprimierung aktiviert oder deaktiviert ist

Bei umfangreichen Workload-Schutz-Plänen sollten Sie einen Testschutz eines typischen Workloads und einige Reproduktionen durchführen und das Ergebnis als Benchmark verwenden, wobei Sie Ihre Metriken während des gesamten Projekts regelmäßig feineinstellen sollten.

1.4.2 Datenkomprimierung

Falls erforderlich, kann PlateSpin Forge die Workload-Daten vor der Übertragung über das Netzwerk komprimieren. So können Sie die Gesamtmenge der während Reproduktionen übertragenen Daten verringern.

Die Komprimierungsverhältnisse hängen von der Art der Dateien auf den Volumes eines Ursprungs-Workloads ab und können von 0,9 (100 MB Daten komprimiert auf 90 MB) bis etwa 0,5 (100 MB komprimiert auf 50 MB) variieren.

Hinweis: Die Datenkomprimierung verwendet die Prozessorleistung des Ursprungs-Workloads.

Die Datenkomprimierung kann pro Schutz oder pro Schutzebene konfiguriert werden. Weitere Informationen hierzu finden Sie in „Schutzebenen“ auf Seite 85.

1.4.3 Bandbreitendrosselung

In PlateSpin Forge können Sie die Menge an verfügbarer Bandbreite, die im Verlauf eines Workload-Schutzes durch die direkte Ursprung-zu-Ziel-Kommunikation verbraucht wird, steuern. Sie können für jeden Schutzplan eine Durchsatzrate festlegen. Dies verhindert, dass Reproduktionsverkehr Ihr Produktionsnetzwerk verstopft, und verringert die Gesamtlast Ihres PlateSpin Forge-Servers.

Bandbreitendrosselung ist ein Parameter in der Schutzebene eines Workload-Schutz-Vertrags. Weitere Informationen hierzu finden Sie in „Schutzebenen“ auf Seite 85.

1.4.4 RPO-, RTO- und TTO-Spezifikationen

- **Angestrebter Wiederherstellungszeitpunkt (RPO):** Beschreibt die akzeptable Menge an Datenverlust, gemessen in Zeit. Der RPO ermittelt sich aus der Zeit zwischen den inkrementellen Reproduktionen eines geschützten Workloads und wird vom aktuellen Nutzungsumfang von PlateSpin Forge, der Rate und dem Ausmaß an Änderungen im Workload sowie von der Netzwerkgeschwindigkeit beeinflusst.
- **Angestrebte Wiederherstellungszeit (RTO):** Beschreibt die Zeit, die für einen Failover-Vorgang (eine Workload-Reproduktion in den Online-Modus versetzen, um einen geschützten Produktions-Workload vorübergehend zu ersetzen) benötigt wird.

  Die für einen Failover eines Workloads auf dessen virtuelle Reproduktion benötigte RTO wird von der Zeit beeinflusst, die für das Konfigurieren und Ausführen des Failover-Vorgangs benötigt wird (10 bis 45 Minuten). Weitere Informationen hierzu finden Sie in „Failover“ auf Seite 65.

- **Angestrebte Testzeit (TTO):** Beschreibt die Zeit, die zum Testen des Wiederherstellungsplans benötigt wird, damit der Dienst erfolgreich wiederhergestellt werden kann.

  Verwenden Sie die Funktion *Failover testen*, um verschiedene Szenarien zu durchlaufen und Vergleichsdaten zu generieren.

Zu den Faktoren, die Auswirkungen auf den RPO sowie die RTO und TTO haben, gehört die Anzahl der erforderlichen gleichzeitigen Failover-Vorgänge. Ein einzelner Failover-Workload beansprucht mehr Arbeitsspeicher und CPU-Ressourcen als mehrere Failover-Workloads, die sich die Ressourcen der ihnen zugrunde liegenden Infrastruktur teilen.

Führen Sie zum Ermitteln der durchschnittlichen Failover-Zeiten für Workloads in Ihrer Umgebung Test-Failovers zu unterschiedlichen Zeiten durch und verwenden Sie diese als Vergleichsdaten in Ihren Gesamtwiederherstellungsplänen. Weitere Informationen hierzu finden Sie in „Generieren von Workload- und Workload-Schutz-Berichten“ auf Seite 57.

Anwendungskonfiguration

2

2.1 Produktlizenzierung

Dieser Abschnitt enthält Informationen für die Aktivierung der PlateSpin Forge-Software.

2.1.1 Abrufen eines Lizenzaktivierungscodes

Für die Produktlizenzierung benötigen Sie einen Lizenzaktivierungscode. Falls Sie nicht über einen Lizenzaktivierungscode verfügen, können Sie diesen über die Novell Customer Center-Website (http://www.novell.com/customercenter/) anfordern. Sie erhalten dann eine Email mit einem Lizenzaktivierungscode.

Wenn Sie sich zum ersten Mal bei PlateSpin Forge anmelden, wird der Browser automatisch zur Seite für die Lizenzaktivierung umgeleitet. Sie haben zwei Möglichkeiten, um Ihre Produktlizenz zu aktivieren: Online-Lizenzaktivierung oder Offline-Lizenzaktivierung.

2.1.2 Online-Lizenzaktivierung

Für die Online-Aktivierung von PlateSpin Forge benötigen Sie einen Internetzugang.

Hinweis: HTTP-Proxys können während der Online-Aktivierung Fehler verursachen. Benutzern in HTTP-Proxy-Umgebungen wird die Offline-Aktivierung empfohlen.

---

1 Klicken Sie im PlateSpin Forge-Web-Client auf *Einstellungen* > *Lizenzen* > *Lizenz hinzufügen*. Die Seite „Lizenzaktivierung“ wird angezeigt.



2 Wählen Sie *Online-Aktivierung*, geben Sie die Email-Adresse, die Sie auch bei der Auftragserteilung angegeben haben, sowie den erhaltenen Aktivierungscode an und klicken Sie anschließend auf *Aktivieren*.

   Das System ruft die erforderliche Lizenz über das Internet ab und aktiviert das Produkt.

2.1.3 Offline-Lizenzaktivierung

Für die Offline-Aktivierung erhalten Sie einen Lizenzschlüssel über das Internet, indem Sie einen Computer mit Internetzugang verwenden.

Hinweis: Sie müssen über ein Novell-Konto verfügen, um einen Lizenzschlüssel abrufen zu können. Wenn Sie bereits PlateSpin-Kunde sind und kein Novell-Konto besitzen, müssen Sie zunächst eines erstellen. Verwenden Sie Ihren bestehenden PlateSpin-Benutzernamen (eine gültige bei PlateSpin registrierte Email-Adresse) als Benutzernamen für Ihr Novell-Konto.

---

1 Klicken Sie auf *Einstellungen* > *Lizenz* und dann auf *Lizenz hinzufügen*. Die Seite „Lizenzaktivierung“ wird angezeigt.
2 Wählen Sie *Offline-Lizenzaktivierung* aus.
3 Verwenden Sie Ihre Hardware-ID, um auf der Website für die PlateSpin Produktaktivierung (http://www.platespin.com/productactivation/ActivateOrder.aspx) eine Lizenzschlüsseldatei zu erstellen. Darüber hinaus werden ein Benutzername, ein Passwort, die Email-Adresse, die Sie bei der Auftragserteilung angegeben haben, und der erhaltene Aktivierungscode benötigt.
4 Geben Sie den Pfad der Datei an oder suchen Sie danach und klicken Sie auf *Aktivieren*.

   Die Lizenzschlüsseldatei wird gespeichert und das Produkt wird basierend auf dieser Datei aktiviert.

2.2 Einrichten der Benutzerautorisierung und -authentifizierung

2.2.1 Info über die Benutzerautorisierung und -authentifizierung von PlateSpin Forge

Der Benutzerautorisierungs- und authentifizierungsmechanismus von PlateSpin Forge basiert auf Benutzerrollen und steuert den Anwendungszugriff sowie die Aktionen, die Benutzer ausführen können. Diesem Mechanismus liegen die Integrierte Windows-Authentifizierung (IWA) und deren Interaktion mit den Internetinformationsdiensten (IIS) zugrunde.

Der rollenbasierte Zugriffsmechanismus bietet Ihnen verschiedene Möglichkeiten, die Autorisierung und Authentifizierung von Benutzern zu implementieren:

- Anwendungszugriff auf bestimmte Benutzer beschränken

- Bestimmte Aktionen nur bestimmten Benutzern erlauben
- Jedem Benutzer Zugriff auf bestimmte Workloads gewähren, um die durch die zugewiesene Rolle definierten Aktionen durchzuführen

Jede PlateSpin Forge-Instanz verfügt auf der Betriebssystemebene über folgende Benutzergruppen, die entsprechende funktionale Rollen definieren:

- **Workload-Schutz-Administratoren:** Besitzen unbegrenzten Zugriff auf alle Funktionen der Anwendung. Ein lokaler Administrator ist implizit Teil dieser Gruppe.
- **Workload-Schutz-Hauptbenutzer:** Besitzen Zugriff auf einen eingeschränkten Teil der Systemfunktionen, und zwar jene, die für die alltägliche Nutzung ausreichen.
- **Workload-Schutz-Operatoren:** Besitzen Zugriff auf die meisten Funktionen der Anwendung, jedoch mit einigen Einschränkungen, z. B. hinsichtlich des Änderns von Systemeinstellungen für die Lizenzierung und Sicherheit.

Wenn ein Benutzer versucht, eine Verbindung mit PlateSpin Forge herzustellen, wird der über den Browser angegebene Berechtigungsnachweis vom IIS geprüft. Wenn der Benutzer keiner der Workload-Schutz-Rollen angehört, wird die Verbindung verweigert. Wenn der Benutzer ein lokaler Administrator auf der Forge-VM ist, wird dieses Konto implizit als Workload-Schutz-Administrator angesehen.

Tabelle 2-1 *Details zu Workload-Schutz-Rollen und -Berechtigungen*

Details zu Workload-Schutz-Rollen	Administratoren	Power-Benutzer	Operatoren
Workload hinzufügen	Zulässig	Zulässig	Verweigert
Workload entfernen	Zulässig	Zulässig	Verweigert
Schutz konfigurieren	Zulässig	Zulässig	Verweigert
Reproduktion vorbereiten	Zulässig	Zulässig	Verweigert
(Voll-)Reproduktion durchführen	Zulässig	Zulässig	Zulässig
Inkrementelle Reproduktion ausführen	Zulässig	Zulässig	Zulässig
Zeitplan unterbrechen/wieder aufnehmen	Zulässig	Zulässig	Zulässig
Failover testen	Zulässig	Zulässig	Zulässig
Failover	Zulässig	Zulässig	Zulässig
Failover abbrechen	Zulässig	Zulässig	Zulässig
Abbrechen	Zulässig	Zulässig	Zulässig
Zurückweisen (Aufgabe)	Zulässig	Zulässig	Zulässig
Einstellungen (Alle)	Zulässig	Verweigert	Verweigert
Berichte/Diagnose ausführen	Zulässig	Zulässig	Zulässig
Failback	Zulässig	Verweigert	Verweigert
Erneut schützen	Zulässig	Zulässig	Verweigert

Darüber hinaus bietet die PlateSpin Forge-Software einen auf *Sicherheitsgruppen* basierenden Mechanismus, der definiert, welche Betriebssystembenutzer auf welche Workloads im Workload-Inventar von PlateSpin Forge zugreifen dürfen.

Das Einrichten eines ordnungsgemäßen rollenbasierten Zugriffs auf PlateSpin Forge umfasst zwei Aufgaben:

1. Hinzufügen von Betriebssystembenutzern zu den erforderlichen, in Tabelle 2-1 aufgeführten Benutzergruppen.
2. Erstellen von Sicherheitsgruppen auf Anwendungsebene, die diese Benutzer bestimmten Workloads zuordnen.

2.2.2 Verwalten von PlateSpin Forge-Zugriff und -Berechtigungen

- „Zugriff auf die Serververwaltungsschnittstelle von PlateSpin Forge“ auf Seite 20
- „Hinzufügen von PlateSpin Forge-Benutzern“ auf Seite 21
- „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Forge-Benutzer“ auf Seite 21
- „Ändern des PlateSpin Forge-Administrator-Passworts“ auf Seite 22

Zugriff auf die Serververwaltungsschnittstelle von PlateSpin Forge

So greifen Sie auf die Web-Benutzerschnittstelle für die Verwaltung von Microsoft Windows-Servern zu:

1 Öffnen Sie einen Webbrowser und gehen Sie zu `https://`*IP-Adresse*`:8098`

Ersetzen Sie *IP-Adresse* durch die IP-Adresse der Forge-VM.

Ihr Browser stellt eine Verbindung zu dem Server her und zeigt die standardmäßige Willkommensseite an.

Abbildung 2-1 *Web-Benutzerschnittstelle für die Verwaltung von Microsoft Windows-Servern*



Hinzufügen von PlateSpin Forge-Benutzern

Gehen Sie wie in diesem Abschnitt beschrieben vor, um einen neuen PlateSpin Forge-Benutzer hinzuzufügen.

Wenn Sie einem auf der Forge-VM vorhandenen Benutzer bestimmte Rollenberechtigungen gewähren möchten, lesen Sie bitte unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Forge-Benutzer“ auf Seite 21 weiter.

1 Öffnen Sie die Web-Benutzerschnittstelle der Serververwaltung von Forge-VM.

   Weitere Informationen hierzu finden Sie unter „Zugriff auf die Serververwaltungsschnittstelle von PlateSpin Forge“ auf Seite 20.

2 Klicken Sie auf *Benutzer* > *Lokale Benutzer*.

   Die Seite „Lokale Benutzer auf dem Server“ wird angezeigt.

3 Klicken Sie unter *Aufgaben* auf *Neu* und geben Sie einen Benutzernamen, ein Passwort und andere optionale Informationen an.

4 Klicken Sie auf *OK*.

   Die Seite „Lokale Benutzer auf dem Server“ wird neu geladen.

Jetzt können Sie dem gerade erstellten Benutzer eine Workload-Schutz-Rolle zuweisen. Weitere Informationen hierzu finden Sie unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Forge-Benutzer“ auf Seite 21.

Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Forge-Benutzer

Bevor Sie einem Benutzer eine Rolle zuweisen, ermitteln Sie, welche Berechtigungen für diesen Benutzer am Besten geeignet sind. Weitere Informationen hierzu finden Sie unter Tabelle 2-1, „Details zu Workload-Schutz-Rollen und -Berechtigungen“, auf Seite 19.

1 Öffnen Sie die Web-Benutzerschnittstelle der Serververwaltung von Forge-VM. Weitere Informationen hierzu finden Sie unter „Zugriff auf die Serververwaltungsschnittstelle von PlateSpin Forge“ auf Seite 20.

2 Klicken Sie auf *Benutzer* > *Lokale Gruppen*.

   Die Seite „Lokale Gruppen auf dem Server“ wird angezeigt.

3 Wählen Sie in der Liste der Gruppen die erforderliche Workload-Schutz-Gruppe aus und klicken Sie anschließend unterhalb von *Aufgaben* auf *Eigenschaften*.

   Die entsprechende Seite mit den Gruppeneigenschaften wird geöffnet.

4 Klicken Sie auf *Mitglieder*, wählen Sie den erforderlichen Benutzer aus der Liste aus und klicken Sie anschließend auf *Hinzufügen*.

   Der ausgewählte Benutzer wird der Liste *Mitglieder* hinzugefügt.

5 Klicken Sie auf *OK*.

Jetzt können Sie diesen Benutzer einer PlateSpin Forge-Sicherheitsgruppe hinzufügen und ihm eine angegebene Sammlung von Workloads zuweisen. Weitere Informationen hierzu finden Sie unter „Verwalten von PlateSpin Forge-Sicherheitsgruppen und -Workload-Berechtigungen“ auf Seite 22.

Ändern des PlateSpin Forge-Administrator-Passworts

So ändern Sie das Passwort des Administratorkontos auf der Forge-VM:

1. Öffnen Sie die Web-Benutzerschnittstelle der Serververwaltung von Forge-VM. Weitere Informationen hierzu finden Sie unter „Zugriff auf die Serververwaltungsschnittstelle von PlateSpin Forge“ auf Seite 20.
2. Klicken Sie auf *Administratorkennwort festlegen*, geben Sie das neue Passwort ein, bestätigen Sie es und klicken Sie anschließend auf *OK*.

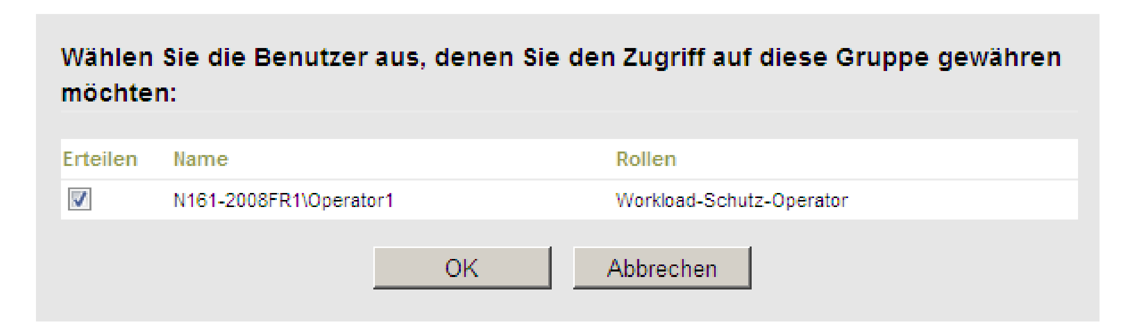
2.2.3 Verwalten von PlateSpin Forge-Sicherheitsgruppen und -Workload-Berechtigungen

PlateSpin Forge bietet auf der Anwendungsebene einen genauer definierten Zugriffsmechanismus, der es bestimmten Benutzern erlaubt, bestimmte Workload-Schutz-Aufgaben für angegebene Workloads durchzuführen. Dies wird durch die Einrichtung von *Sicherheitsgruppen* erreicht.

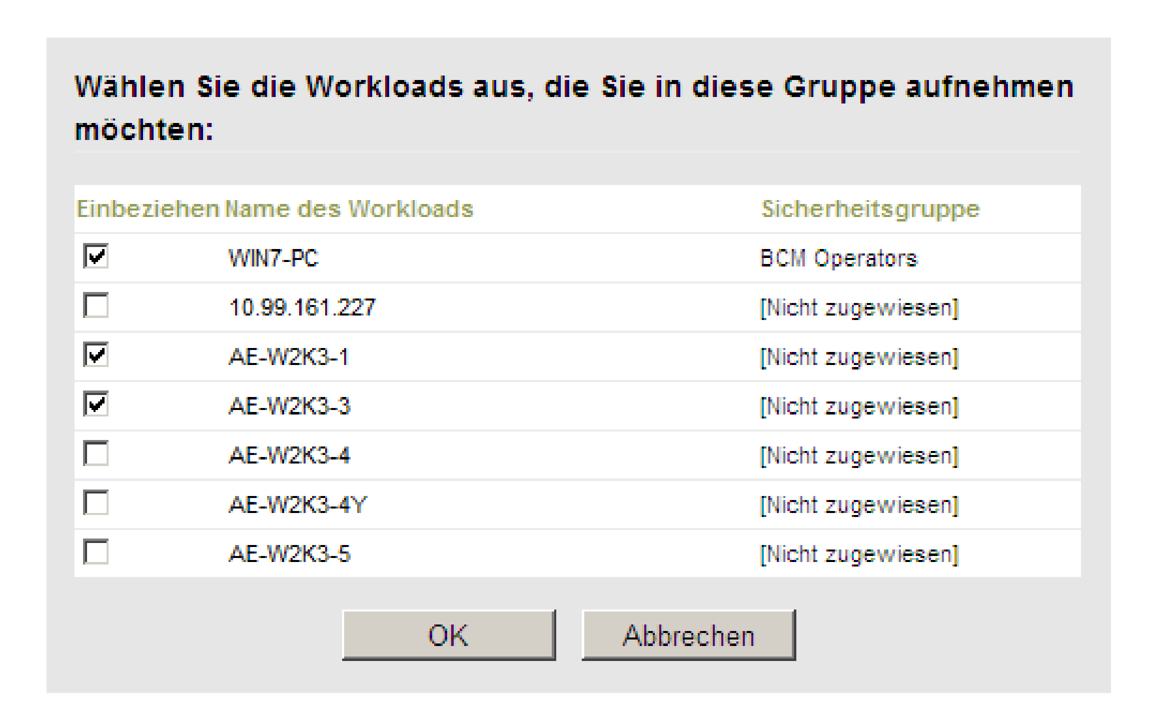
1. Weisen Sie einem PlateSpin Forge-Benutzer die Workload-Schutz-Rolle zu, deren Berechtigungen am besten für die Rolle dieses Benutzers in Ihrer Organisation geeignet sind. Weitere Informationen hierzu finden Sie unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Forge-Benutzer“ auf Seite 21.
2. Greifen Sie als Administrator über den PlateSpin Forge-Web-Client auf PlateSpin Forge zu und klicken Sie anschließend auf *Einstellungen* > *Berechtigungen*.

   Die Seite „Sicherheitsgruppen“ wird angezeigt:
3. Klicken Sie auf *Sicherheitsgruppe erstellen*.
4. Geben Sie im Feld *Name der Sicherheitsgruppe* einen Namen für Ihre Sicherheitsgruppe ein.
5. Klicken Sie auf *Benutzer hinzufügen* und wählen Sie die erforderlichen Benutzer für diese Sicherheitsgruppe aus.

   Wenn Sie einen PlateSpin Forge-Benutzer hinzufügen möchten, der kürzlich als Benutzer auf Betriebssystemebene zur Forge-VM hinzugefügt wurde, wird er möglicherweise nicht sofort in der Benutzeroberfläche angezeigt. Klicken Sie in diesem Fall auf *Benutzerkonten aktualisieren*.



6. Klicken Sie auf *Workload hinzufügen* und wählen Sie die erforderlichen Workloads aus:



Nur die Benutzer in dieser Sicherheitsgruppe haben Zugriff auf die ausgewählten Workloads.

7 Klicken Sie auf *Erstellen*.

Die Seite wird neu geladen und zeigt Ihre neue Gruppe in der Liste der Sicherheitsgruppen an.

Wenn Sie eine Sicherheitsgruppe bearbeiten möchten, klicken Sie in der Liste der Sicherheitsgruppen auf ihren Namen.

2.3 Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk

- Abschnitt 2.3.1, „Zugriffs- und Kommunikationsanforderungen für Workloads“, auf Seite 23
- Abschnitt 2.3.2, „Schutz über öffentliche und private Netzwerke durch NAT“, auf Seite 25

2.3.1 Zugriffs- und Kommunikationsanforderungen für Workloads

Nachfolgend werden die Software-, Netzwerk- und Firewall-Anforderungen für Workloads beschrieben, die mithilfe von PlateSpin Forge geschützt werden sollen.

Tabelle 2-2 *Zugriffs- und Kommunikationsanforderungen für Workloads*

Workload-Typ	Voraussetzungen	Erforderliche Ports
Alle Workloads	Ping-Funktion (ICMP-Echoanfrage und -antwort).	
Alle Windows-Workloads	.NET Framework Version 2.0 oder höher	

<table>
<tr><th>Workload-Typ</th><th>Voraussetzungen</th><th>Erforderliche Ports</th></tr>
<tr><td>Windows 7;

Windows Server 2008;

Windows Vista</td><td>Integrierte <code>Administrator</code>- oder Domänen-Administrator-Kontoberechtigungsnachweise (die Mitgliedschaft in der lokalen Administratorgruppe reicht nicht aus). Unter Vista muss das Konto aktiviert sein (es ist standardmäßig deaktiviert).
Bei der Konfiguration der Windows-Firewall müssen die folgenden Eingangsregeln aktiviert und auf <code>Zulassen</code> gesetzt werden:
Datei- und Druckerfreigabe (Echoanforderung - ICMPv4In)
Datei- und Druckerfreigabe (Echoanforderung - ICMPv6In)
Datei- und Druckerfreigabe (NB-Datagramm eingehend)
Datei- und Druckerfreigabe (NB-Name eingehend)
Datei- und Druckerfreigabe (NB-Sitzung eingehend)
Datei- und Druckerfreigabe (SMB eingehend)
Datei- und Druckerfreigabe (Spoolerdienst - RPC)
Datei- und Druckerfreigabe (Spoolerdienst - RPC-EPMAP)
Diese Firewall-Einstellungen werden mithilfe der Windows-Firewall mit dem Dienstprogramm „Erweiterte Sicherheit“ (<code>wf.msc</code>) konfiguriert. Sie können dasselbe Ergebnis erzielen, indem Sie das grundlegende Windows-Firewall-Dienstprogramm (<code>firewall.cpl</code>) verwenden. Wählen Sie in der Liste der Ausnahmen das Element Datei- und Druckerfreigabe aus.</td><td>TCP 3725

NetBIOS 137 - 139

SMB (TCP 139, 445 und UDP 137, 138)

TCP 135/445</td></tr>
</table>

Workload-Typ	Voraussetzungen	Erforderliche Ports
Windows Server 2000; Windows XP; Windows NT 4	◆ Installierte Windows Management Instrumentation (WMI) Bei Windows NT Server gehört WMI nicht zur Standardinstallation. Sie können den WMI Core von der Microsoft-Website beziehen. Wenn WMI nicht installiert ist, schlägt die Ermittlung des Workloads fehl. WMI (RPC/DCOM) kann die TCP-Ports 135 und 445 sowie zufällig oder dynamisch zugewiesene Ports oberhalb von 1024 verwenden. Falls während des Ermittlungsvorgangs Probleme auftreten, sollten Sie den Workload vorübergehend in eine DMZ platzieren oder die durch eine Firewall geschützten Ports vorübergehend für die Ermittlung öffnen. Weitere Informationen, z. B. eine Anleitung für das Beschränken des Portbereichs für DCOM und RPC, finden Sie in den folgenden technischen Artikeln von Microsoft. ◆ Verwenden von DCOM mit Firewalls (http://msdn.microsoft.com/en-us/library/ms809327.aspx) ◆ Konfigurieren der dynamischen RPC-Port-Zuordnung für die Verwendung mit Firewalls (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) ◆ Konfigurieren von DCOM für die Verwendung mit einer NAT-basierten Firewall (http://support.microsoft.com/kb/248809)	TCP 3725 NetBIOS 137 - 139 SMB (TCP 139, 445 und UDP 137, 138) TCP 135/445
Alle Linux-Workloads	Secure Shell (SSH)-Server	TCP 22, 3725

2.3.2 Schutz über öffentliche und private Netzwerke durch NAT

In einigen Fällen kann sich ein Ursprung, ein Ziel oder PlateSpin Forge selbst in einem internen (privaten) Netzwerk hinter einem NAT-Gerät (Network Address Translator) befinden, wodurch eine Kommunikation mit dem Gegenstück während des Schutzes nicht möglich ist.

PlateSpin Forge ermöglicht Ihnen, dieses Problem zu umgehen, je nachdem, welcher der folgenden Hosts sich hinter dem NAT-Gerät befindet:

- **PlateSpin Forge-Server:** Fügen Sie die diesem Host zugewiesenen zusätzlichen IP-Adressen zur Konfigurationsdatei `web.config` Ihres Servers hinzu. Weitere Informationen hierzu finden Sie in „Parameter für zusätzliche IP-Adressen des PlateSpin Forge-Servers (NAT-Einstellungen)“ auf Seite 32.
- **Quell-Workload:** Wird nur für Failback unterstützt, wo Sie eine alternative IP-Adresse für den Wiederherstellungs-Workload in Failback-Details (Workload an VM) (Seite 70) angeben können.
- **Failback-Ziel:** Wenn Sie versuchen, ein Failback-Ziel zu registrieren, geben Sie die öffentliche (oder externe) IP-Adresse in den Parametern für die Ermittlung/Registrierung an.

2.4 Konfigurieren von PlateSpin Forge-Standardoptionen

2.4.1 Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten

Sie können PlateSpin Forge so konfigurieren, dass es automatisch Benachrichtigungen zu Ereignissen und Reproduktionsberichte an angegebene Email-Adressen sendet. Für diese Funktion ist es erforderlich, dass Sie zuerst einen gültigen SMTP-Server für PlateSpin Forge angeben.

SMTP-Konfiguration

Verwenden Sie den PlateSpin Forge-Web-Client, um die SMTP-Einstellungen für den Server zu konfigurieren, der zum Zustellen von Email-Benachrichtigungen zu Ereignissen und Reproduktionsberichten verwendet wird.

Abbildung 2-2 *SMTP-Einstellungen (Simple Mail Transfer Protocol)*



So konfigurieren Sie die SMTP-Einstellungen:

1. Klicken Sie im PlateSpin Forge-Web-Client auf *Einstellungen* > *SMTP*.
2. Geben Sie die *Adresse* und den *Port* (Standardport ist 25) Ihres SMTP-Servers sowie eine *Antwortadresse* für den Empfang von Email-Benachrichtigungen zu Ereignissen und zum Fortschritt an.
3. Geben Sie den *Benutzernamen* und das *Passwort* ein. Bestätigen Sie anschließend das Passwort.
4. Klicken Sie auf *Speichern*.

Einrichten automatischer Ereignisbenachrichtigungen per Email

1. Richten Sie einen SMTP-Server für PlateSpin Forge ein. Weitere Informationen hierzu finden Sie in SMTP-Konfiguration.
2. Klicken Sie im PlateSpin Forge-Web-Client auf *Einstellungen* > *Email* > *Benachrichtigungen*.
3. Wählen Sie die Option *Benachrichtigungen aktivieren*.
4. Klicken Sie auf *Empfänger bearbeiten*, geben Sie die erforderlichen Email-Adressen getrennt durch Kommas ein und klicken Sie anschließend auf *OK*.
5. Klicken Sie auf *Speichern*.

   Klicken Sie zum Löschen aufgelisteter Email-Adressen auf *Löschen* neben den zu entfernenden Adressen.

Folgende Ereignisse lösen E-Mail-Benachrichtigungen aus:

Ereignis	Anmerkungen
`Workload online erkannt`	Wird generiert, wenn das System erkennt, dass ein Workload, der zuvor offline war, nun online ist. Betrifft Workloads, deren Schutzzeitplan-Status nicht *Unterbrochen* lautet.
`Workload offline erkannt`	Wird generiert, wenn das System erkennt, dass ein Workload, der zuvor online war, nun offline ist. Betrifft Workloads, deren Schutzzeitplan-Status nicht *Unterbrochen* lautet.
`Fehler bei der inkrementellen Reproduktion`	
`Fehler bei der Vollreproduktion`	
`Failover-Test abgeschlossen`	Wird generiert, wenn ein Failover-Test-Vorgang manuell als ordnungsgemäß durchgeführt oder als Fehler gekennzeichnet wird.
`Failover abgeschlossen`	
`Failover-Vorbereitung abgeschlossen`	
`Failover-Vorbereitung fehlgeschlagen`	
`Failover-Fehler`	

Ereignis	Anmerkungen
`Inkrementelle Reproduktion verpasst`	Wird in folgenden Fällen generiert: ◆ Eine Reproduktion wird manuell angehalten, wenn eine geplante inkrementelle Reproduktion fällig ist. ◆ Das System versucht, eine geplante inkrementelle Reproduktion auszuführen, während gerade eine manuell ausgelöste Reproduktion stattfindet. ◆ Das System stellt fest, dass das Ziel nicht über genügend freien Speicherplatz verfügt.
`Vollreproduktion verpasst`	Ähnlich dem Ereignis `Inkrementelle Reproduktion verpasst` weiter oben.

Einrichten automatischer Reproduktionsberichte per Email

Führen Sie folgende Schritte aus, um PlateSpin Forge so einzurichten, dass es automatisch Reproduktionsberichte per Email sendet:

1. Richten Sie einen SMTP-Server für PlateSpin Forge ein. Weitere Informationen hierzu finden Sie in SMTP-Konfiguration.
2. Klicken Sie im PlateSpin Forge-Web-Client auf *Einstellungen* > *Email* > *Reproduktionsberichte*.
3. Wählen Sie die Option *Reproduktionsberichte aktivieren*.
4. Klicken Sie im Abschnitt *Berichtswiederholung* auf *Konfigurieren* und geben Sie das erforderliche Wiederholungsmuster für die Berichte an.
5. Klicken Sie im Abschnitt *Empfänger* auf *Empfänger bearbeiten*, geben Sie die erforderlichen Email-Adressen getrennt durch Kommas ein und klicken Sie anschließend auf *OK*.
6. (Optional) Geben Sie im Abschnitt *Protect-Zugriff-URL* eine nicht standardmäßige URL für Ihren PlateSpin Forge-Server ein (z. B. wenn Ihre Forge-VM mehrere Netzwerkkarten hat oder sich hinter einem NAT-Server befindet). Diese URL hat Einfluss auf den Titel des Berichts und auf die Funktionalität für den Zugriff auf relevante Inhalte auf dem Server über Hyperlinks in Email-Berichten.
7. Klicken Sie auf *Speichern*.

Informationen zu anderen Arten von Berichten, die Sie jederzeit generieren können, finden Sie unter „Generieren von Workload- und Workload-Schutz-Berichten“ auf Seite 57.

2.4.2 Einrichtung der Sprache bei internationalen Versionen von PlateSpin Forge

PlateSpin Forge bietet Unterstützung von Landessprachen (NLS, National Language Support) für Chinesisch (vereinfacht), Chinesisch (traditionell), Französisch, Deutsch und Japanisch.

Zur Verwendung des PlateSpin Forge-Web-Clients und der integrierten Hilfe in einer dieser Sprachen muss die entsprechende Sprache in Ihrem Webbrowser hinzugefügt und an die erste Position der Rangfolge gesetzt werden:

1. Rufen Sie in Ihrem Webbrowser die Spracheinstellung auf:
   - **Internet Explorer:** Klicken Sie auf *Extras* > *Internetoptionen* > *Registerkarte „Allgemein“* > *Sprachen*.
   - **Firefox:** Klicken Sie auf *Extras* > *Einstellungen* > *Registerkarte „Inhalt“* > *Sprachen*.
2. Fügen Sie die gewünschte Sprache hinzu und setzen Sie sie an die oberste Position in der Liste.
3. Speichern Sie die Einstellungen und starten Sie anschließend die Client-Anwendung, indem Sie eine Verbindung zu Ihrem PlateSpin Forge-Server herstellen. Weitere Informationen hierzu finden Sie in „Starten des PlateSpin Forge-Web-Clients“ auf Seite 49.

Hinweis: (Für Benutzer der chinesischen Versionen) Der Versuch, über einen Browser ohne spezifische chinesische Version eine Verbindung zum PlateSpin Forge Server herzustellen, kann zu Webserver-Fehlern führen. Verwenden Sie für den ordnungsgemäßen Betrieb die Konfigurationseinstellungen des Browsers, um eine spezifische chinesische Spracheinstellung hinzuzufügen (`Chinesisch [zh-cn]` oder `Chinesisch [zh-tw]`). Verwenden Sie die kulturneutrale Spracheinstellung `Chinesisch [zh]` nicht.

Die Sprache eines geringen Anteils der vom PlateSpin Forge-Server generierten Systemmeldungen hängt von der Sprache der Betriebssystemschnittstelle ab, die in Ihrer Forge-VM ausgewählt ist:

1. Rufen Sie Ihre Forge-VM auf.

   Weitere Informationen hierzu finden Sie in Abschnitt 3.4.1, „Forge Management-VM im Appliance-Host - Zugriff und Verwendung“, auf Seite 41.
2. Starten Sie das Applet für die Regions- und Sprachoptionen (klicken Sie auf *Start* > *Ausführen*, geben Sie `intl.cpl` ein und drücken Sie die Eingabetaste) und klicken Sie anschließend auf die Registerkarte *Sprachen* (Windows Server 2003) bzw. *Tastaturen und Sprachen* (Windows Server 2008).
3. Installieren Sie das erforderliche Sprachpaket, sofern es noch nicht installiert ist. Möglicherweise benötigen Sie Zugriff auf die Installationsmedien Ihres Betriebssystems.
4. Wählen Sie die erforderliche Sprache als Oberflächensprache des Betriebssystems aus. Wenn eine entsprechende Aufforderung angezeigt wird, melden Sie sich ab oder starten Sie das System neu.

2.4.3 Konfigurieren des Produktverhaltens mithilfe von XML-Konfigurationsparametern

Bestimmte Aspekte des Verhaltens des PlateSpin Forge Servers PlateSpin Forge-Servers werden von Konfigurationsparametern gesteuert, die aus `*.config`-Dateien auf Ihrer Forge-VM gelesen werden.

Normalerweise brauchen Sie diese Einstellungen nicht zu ändern, es sei denn, der PlateSpin-Support rät Ihnen dazu. In diesem Abschnitt werden einige häufig vorkommende Fälle zusammen mit Informationen zur erforderlichen Prozedur aufgeführt.

Gehen Sie wie folgt vor, um `*.config`-Parameter zu ändern oder anzuwenden:

1. Navigieren Sie auf der Forge-VM zum angegebenen Verzeichnis.
2. Öffnen Sie die `*.config`-Datei in einem Texteditor.
3. Wählen Sie den entsprechenden Parameter in der `.config`-Datei aus und ändern Sie dessen Wert. Der Wert ist in Anführungszeichen (" ") gesetzt. Löschen Sie nicht die Anführungszeichen. Verwenden Sie vertretbare Werte, wie in diesem Abschnitt angegeben, bzw. die Werte, die vom PlateSpin-Support angegeben werden.
4. Speichern und schließen Sie die `*.config`-Datei.
5. Starten Sie den PlateSpin Forge-Server neu. Weitere Informationen hierzu finden Sie unter „Neustart des PlateSpin Forge-Servers, um Systemänderungen anzuwenden“ auf Seite 32.

Die folgenden Themen bieten Informationen zu häufig verwendeten Konfigurationsdateien und Werten, die sich auf das Verhalten Ihres PlateSpin Forge-Servers auswirken.

Parameter für die Optimierung von Übertragungen in WAN-Verbindungen

Mit diesen Einstellungen können Sie Übertragungen in einem WAN optimieren. Diese globalen Einstellungen gelten für alle dateibasierten und VSS-Reproduktionen.

- **Konfigurationsdatei:** `productinternal.config`
- **Standort:** `Programme\PlateSpin Forge Server\Web`

Weitere Informationen zum Aktualisierungsvorgang finden Sie unter „Konfigurieren des Produktverhaltens mithilfe von XML-Konfigurationsparametern“ auf Seite 29.

Hinweis: Wenn Sie diese Werte ändern, beeinträchtigt dies möglicherweise die Geschwindigkeit bei Reproduktionen im LAN.

In Tabelle 2-3 sind die Konfigurationsparameter in zwei Gruppen aufgeführt: die Standardwerte und die Werte, die für den optimalen Betrieb in einer WAN-Umgebung mit hoher Latenz empfohlen werden.

Tabelle 2-3 *Standard- und optimale Konfigurationsparameter in* `productinternal.config`

Parameter	Standardwert	Optimaler Wert
`fileTransferThreadcount` Steuert die Anzahl der TCP-Verbindungen, die für den dateibasierten Datentransfer geöffnet werden.	2	4 bis 6

Parameter	Standardwert	Optimaler Wert
`fileTransferMinCompressionLimit` Gibt den Schwellwert für die Komprimierung auf Paketebene in Byte an.	0 (deaktiviert)	Max. 65536 (64 KB)
`fileTransferCompressionThreadsCount` Steuert die Anzahl der Threads, die für die Datenkomprimierung auf Paketebene verwendet werden. Wird ignoriert, wenn die Komprimierung deaktiviert ist. Da die Komprimierung CPU-abhängig ist, kann sich diese Einstellung auf die Arbeitsgeschwindigkeit auswirken.	2	nicht zutreffend

`fileTransferSendReceiveBufferSize`
 	
Einstellung der TCP/IP-Fenstergröße für Dateiübertragungsverbindungen. Sie steuert die Anzahl der Byte, die ohne TCP-Acknowledgement gesendet werden. Angabe in Byte.
 	
Wenn der Wert auf 0 gesetzt wird, wird die Standard-TCP-Fenstergröße (8 KB) verwendet. Geben Sie bei benutzerdefinierten Größen die Größe in Byte an. Verwenden Sie folgende Formel, um den geeigneten Wert zu ermitteln:
 	
((Verbindungsgeschwindigkeit(MB/s)/8)*Verzögerung(Sek.))*1000*1000
 	
Beispielsweise wäre die geeignete Puffergröße bei einer 100-Mb/s-Verbindung mit 10 ms Latenz wie folgt:
 	
`(100/8)*0,01 * 1000 * 1000 = 125000 Byte`
	0 (8192 Byte)	Max. 5242880 (5 MB)

Parameter für das Aktivieren der SSL-Kommunikation

Verwenden Sie diese Einstellungen, um die SSL-Kommunikation zwischen dem PlateSpin Forge-Web-Client und dem Server, auf dem Sie SSL aktiviert haben, *nach* der Installation des Produkts zu aktivieren. Wenn SSL zum Zeitpunkt der Produktinstallation auf dem Server-Host aktiviert war, ist dies nicht erforderlich.

- **Konfigurationsdatei:** `Platespin.Config`
- **Standort:** `Programme\PlateSpin Forge Server\Configs`
- **Wert:** Änderung

  ```
  <add key="PowerConvertURL" value="http://localhost:80/PlateSpinMigrate" />
  ```

  in

  ```
  <add key="PowerConvertURL" value="https://localhost:443/PlateSpinMigrate"
  />
  ```

Weitere Informationen zum Aktualisierungsvorgang finden Sie unter „Konfigurieren des Produktverhaltens mithilfe von XML-Konfigurationsparametern“ auf Seite 29.

Parameter zum Auferlegen eines Reproduktionssperrzeitfensters

- **Konfigurationsdatei:** `PlateSpin.Protection.Scheduler.Service.dll.config`
- **Standort:** `Programme\PlateSpin Forge Server\services\PlateSpinService\Plugins`
- **Werte:** Dieser Parameter umfasst zwei Werte:
  - `Workload_Scheduling_Blackout_Window_Start`: Legt die Startzeit für das Aussetzen der Reproduktion fest. Verwenden Sie das folgende Format:

    `HH:MM:SS (HH 00-23, MM 00-59, SS 00-59)`
  - `Workload_Scheduling_Blackout_Window_Length`: Legt die Dauer des Aussetzens der Reproduktion fest. Verwenden Sie das folgende Format:

    `HH:MM:SS (HH 00-23, MM 00-59, SS 00-59)`

Weitere Informationen zum Aktualisierungsvorgang finden Sie unter „Konfigurieren des Produktverhaltens mithilfe von XML-Konfigurationsparametern“ auf Seite 29.

Parameter für zusätzliche IP-Adressen des PlateSpin Forge-Servers (NAT-Einstellungen)

Verwenden Sie diese Einstellungen, um zusätzliche IP-Adressen Ihres PlateSpin Forge-Servers für die Kommunikation in NAT-fähigen Umgebungen anzugeben:

- **Konfigurationsdatei:** `Web.config`
- **Standort:** `Programme\PlateSpin Forge Server\Web`
- **Werte:** `<add key="AlternateServerAddresses" value="" />`

  Fügen Sie die zusätzlichen IP-Adressen getrennt durch Semicolons (;) hinzu, z. B.:

  `<add key="AlternateServerAddresses" value="10.99.106.108;10.99.106.109" />`

2.4.4 Neustart des PlateSpin Forge-Servers, um Systemänderungen anzuwenden

1. Navigieren Sie zum PlateSpin Forge-Server-Unterverzeichnis `bin\RestartPlateSpinServer`.

   Weitere Informationen hierzu finden Sie in Abschnitt 3.4.1, „Forge Management-VM im Appliance-Host - Zugriff und Verwendung“, auf Seite 41.
2. Doppelklicken Sie auf die Programmdatei `RestartPlateSpinServer.exe`.

   Es wird ein Befehlszeilenfenster geöffnet, in dem Sie aufgefordert werden, den Vorgang zu bestätigen.
3. Geben Sie `Y` ein und drücken Sie die `Eingabetaste`.

Appliance-Einrichtung und Wartung

3

Dieser Abschnitt enthält Informationen zu Einrichtungs- und Wartungsaufgaben für die Appliance, die Sie möglicherweise regelmäßig ausführen müssen.

- Abschnitt 3.1, „Einrichten des Appliance-Netzwerks“, auf Seite 33
- Abschnitt 3.2, „Standortänderung der PlateSpin Forge-Appliance und Neuzuweisung der IP-Adressen“, auf Seite 34
- Abschnitt 3.3, „Verwenden externer Speicherlösungen mit PlateSpin Forge“, auf Seite 39
- Abschnitt 3.4, „Wartung der PlateSpin Forge-Appliance“, auf Seite 41
- Abschnitt 3.5, „Aufrüsten von PlateSpin Forge“, auf Seite 46

3.1 Einrichten des Appliance-Netzwerks

Dieses Kapitel bietet Informationen zum Anpassen der Netzwerkeinstellungen des Appliance-Hosts.

- Abschnitt 3.1.1, „Einrichten des Appliance-Host-Netzwerks“, auf Seite 33

3.1.1 Einrichten des Appliance-Host-Netzwerks

Die PlateSpin Forge-Appliance verfügt über sechs für den externen Zugriff konfigurierte physische Netzwerkschnittstellen:

- **Externes Testnetzwerk:** Dient der Isolierung des Netzwerkdatenverkehrs beim Testen eines Failover-Workloads mit der Funktion „Failover testen“.
- **Internes Testnetzwerk:** Zum Testen eines Failover-Workloads in völliger Isolation vom Produktionsnetzwerk.
- **Reproduktionsnetzwerk:** Bereitstellung eines Netzwerks für das System, das dem laufenden Datenverkehr zwischen dem Produktions-Workload und seiner Reproduktion in der Management-VM vorbehalten ist.
- **Produktionsnetzwerk:** Dient der Fortführung der realen Geschäftsprozesse, wenn ein Failover oder ein Failback durchgeführt wird.
- **Management-Netzwerk:** Das Forge Management-VM-Netzwerk.
- **Appliance-Host-Netzwerk:** Hypervisor-Management-Netzwerk. Im PlateSpin Forge-Web-Client steht dieses Netzwerk nicht zur Auswahl.

Zum Standardlieferumfang von PlateSpin Forge gehören alle sechs physischen Netzwerkschnittstellen, die einem einzelnen vSwitch im Hypervisor zugeordnet sind. Sie können die Zuordnung gemäß den Anforderungen Ihrer Umgebung entsprechend anpassen. Sie können beispielsweise einen Workload mit zwei Netzwerkkarten schützen, wobei eine Netzwerkarte für die Produktionskonnektivität und die andere ausschließlich für Reproduktionen verwendet werden. Weitere Informationen hierzu finden Sie im KB-Beitrag 7921062 (http://www.novell.com/support/viewContent.do?externalId=7921062).

Darüber hinaus können Sie jeder dieser einzelnen Portgruppen unterschiedliche VLAN-IDs zuweisen, um die Steuerung des Netzwerkdatenverkehrs ausgefeilter abzustimmen. Dadurch wird sichergestellt, dass das Produktionsnetzwerk nicht von dem Datenverkehr der Workload-Schutz- und Wiederherstellungsvorgänge gestört wird. Weitere Informationen hierzu finden Sie im KB-Artikel 21057 (http://www.novell.com/support/viewContent.do?externalId=7921057).

3.2 Standortänderung der PlateSpin Forge-Appliance und Neuzuweisung der IP-Adressen

Eine Änderung des Standorts Ihrer PlateSpin Forge-Appliance erfordert eine Änderung der IP-Adressen ihrer Komponenten, um die neue Umgebung zu reflektieren. Dies sind die IP-Adressen, die Sie während der anfänglichen Einrichtung der Appliance angegeben haben (siehe *Handbuch mit ersten Schritten zu Forge*).

Die Vorgehensweise hängt von der *Appliance-Version* (1 oder 2) ab. Informationen über das Ermitteln der Appliance-Version Ihrer Einheit finden Sie unter *Ermitteln der Appliance-Version Ihrer Einheit* im Handbuch *Forge - Erste Schritte*.

- Abschnitt 3.2.1, „Standortänderung der Forge-Appliance Version 2“, auf Seite 34
- Abschnitt 3.2.2, „Standortänderung der Forge-Appliance Version 1“, auf Seite 38

3.2.1 Standortänderung der Forge-Appliance Version 2

Vor Beginn der Standortänderung:

1. Unterbrechen Sie alle Reproduktionszeitpläne. Stellen Sie dabei sicher, dass mindestens eine inkrementelle Reproduktion für jeden Workload ausgeführt wurde:
   - **1a** Wählen Sie im Web-Client der PlateSpin Forge-Appliance alle Workloads aus, klicken Sie auf *Unterbrechen* und anschließend auf *Ausführen*.
   - **1b** Stellen Sie sicher, dass der Status *Unterbrochen* für alle Workloads angezeigt wird.

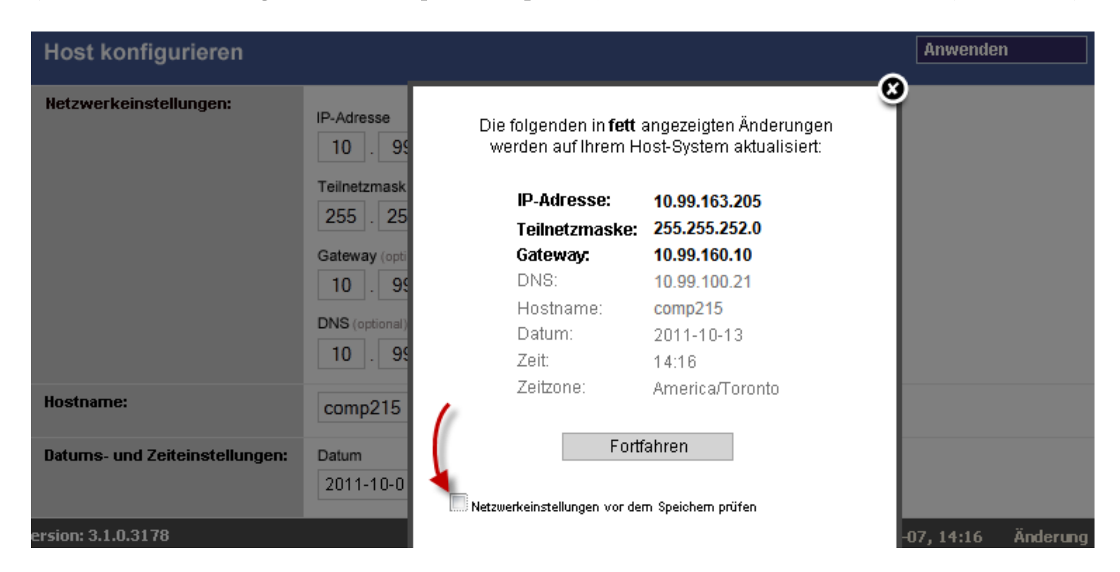
Die Vorgehensweise für die Standortänderung hängt davon ab, ob die neue IP-Adresse der Appliance am Zielstandort bekannt (Szenario 1) oder nicht bekannt (Szenario 2) ist.

- „Szenario 1 - Standortänderung der Forge-Appliance (neue IP-Adresse bekannt)“ auf Seite 34
- „Szenario 2 - Standortänderung der Forge-Appliance (neue IP-Adresse nicht bekannt)“ auf Seite 36

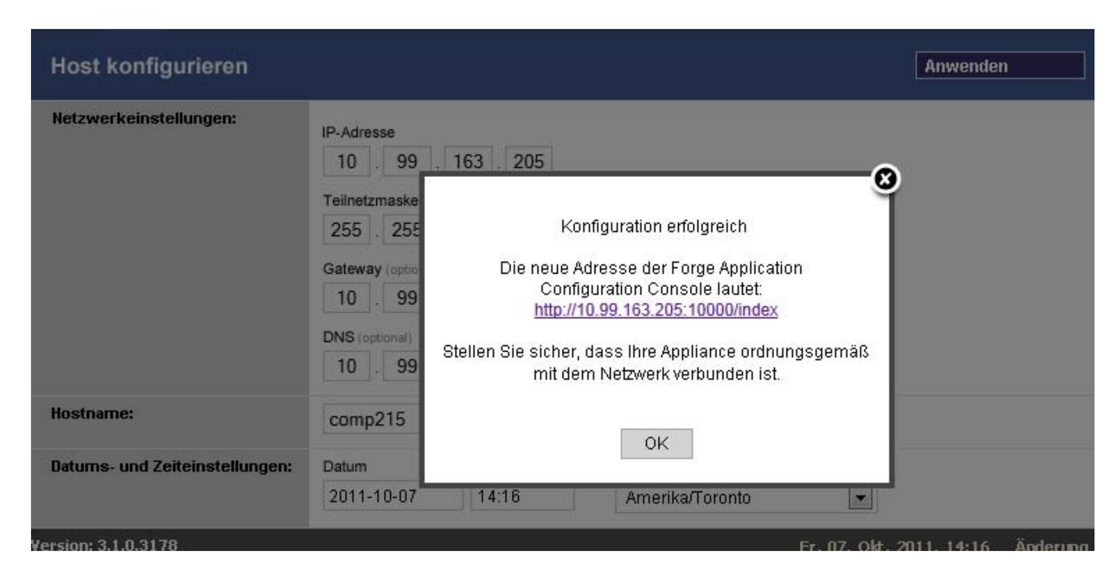
Szenario 1 - Standortänderung der Forge-Appliance (neue IP-Adresse bekannt)

1. Unterbrechen Sie alle Reproduktionen. Weitere Informationen hierzu finden Sie unter Schritt 1a und Schritt 1b oben.
2. Starten Sie die Forge Appliance Configuration Console (ACC): Öffnen Sie einen Browser und navigieren Sie zu `http://<Forge_IP_Adresse>:10000`.
3. Melden Sie sich mit dem `forgeuser`-Konto an und klicken Sie auf *Configure Host* (Host konfigurieren).
4. Geben Sie die neuen Netzwerkeinstellungen ein und klicken Sie auf *Anwenden*.

5 Vergewissern Sie sich, dass die im Bestätigungsfenster angezeigten neuen Einstellungen korrekt sind. Deaktivieren Sie die Option *Verify network settings before saving* (Netzwerkeinstellungen vor dem Speichern prüfen) und klicken Sie auf *Continue* (Fortfahren).



6 Warten Sie, bis der Konfigurationsvorgang abgeschlossen ist und im Browser das Meldungsfenster „Configuration Successful“ (Konfiguration erfolgreich) geöffnet wird.



Hinweis: Der Link für die neue ACC-Adresse im Meldungsfenster funktioniert erst, nachdem Sie die Appliance physisch getrennt und an das neue Teilnetz angeschlossen haben.

---

7 Fahren Sie die Appliance herunter:

7a Fahren Sie die Forge Management-VM herunter. Weitere Informationen hierzu finden Sie unter „Starten und Herunterfahren der Forge Management-VM“ auf Seite 44.

7b Fahren Sie den Appliance-Host herunter:

7b1 Drücken Sie an der Forge-Konsole „Alt-F2“, um zur ESX-Serverkonsole zu wechseln.

7b2 Melden Sie sich als „superuser“ an (Benutzer `root` und das zugehörige Passwort).

7b3 Geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
shutdown -h now
```

7c Schalten Sie die Appliance aus.

8 Trennen Sie die Appliance und stellen Sie sie am neuen Standort auf. Verbinden Sie die Appliance mit dem neuen Teilnetz und schalten Sie sie ein.

Die neue IP-Adresse sollte jetzt gültig sein.

9 Starten Sie die ACC und melden Sie sich mit dem `forgeuser`-Konto an. Klicken Sie auf *Configure Forge VM* (Forge-VM konfigurieren), geben Sie die erforderlichen Parameter an und klicken Sie auf *Anwenden*.

10 Vergewissern Sie sich, dass die Einstellungen korrekt sind, klicken Sie auf *Continue* (Fortfahren) und warten Sie, bis der Vorgang abgeschlossen ist.

Hinweis: Wenn die Forge-VM für DHCP eingerichtet wurde, führen Sie nach der Standortänderung die folgenden Schritte aus:

1. Ermitteln Sie die neue IP-Adresse der Forge-VM (greifen Sie mithilfe des VMware-Clients auf die Forge-VM zu und suchen Sie die Adresse in der Windows-Schnittstelle der VM. Weitere Informationen hierzu finden Sie in „Starten des VMware-Clients und Zugriff auf die Forge Management-VM“ auf Seite 42).

2. Verwenden Sie die neue IP-Adresse, um den PlateSpin Forge-Web-Client zu starten, und aktualisieren Sie den Container (klicken Sie auf *Einstellungen* > *Container* > *und anschließend auf das Symbol*).

---

11 Setzen Sie die angehaltenen Reproduktionen fort.

Szenario 2 - Standortänderung der Forge-Appliance (neue IP-Adresse nicht bekannt)

1 Unterbrechen Sie alle Reproduktionen. Weitere Informationen hierzu finden Sie in Schritt 1 auf Seite 34.

2 Fahren Sie die Appliance herunter:

2a Fahren Sie die Forge Management-VM herunter. Weitere Informationen hierzu finden Sie unter „Starten und Herunterfahren der Forge Management-VM“ auf Seite 44.

2b Fahren Sie den Appliance-Host herunter:

2b1 Drücken Sie an der Forge-Konsole „Alt-F2“ , um zur ESX-Serverkonsole zu wechseln.

2b2 Melden Sie sich als „superuser“ an (Benutzer `root` und das zugehörige Passwort).

2b3 Geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
shutdown -h now
```

2c Schalten Sie die Appliance aus.

3 Trennen Sie die Appliance und stellen Sie sie am neuen Standort auf. Verbinden Sie die Appliance mit dem neuen Netzwerk und schalten Sie sie ein.

4 Richten Sie einen Computer (Notebook empfohlen) so ein, dass er mit Forge über die aktuelle IP-Adresse (die IP-Adresse am alten Standort) kommunizieren kann. Schließen Sie anschließend den Computer an der Appliance an.

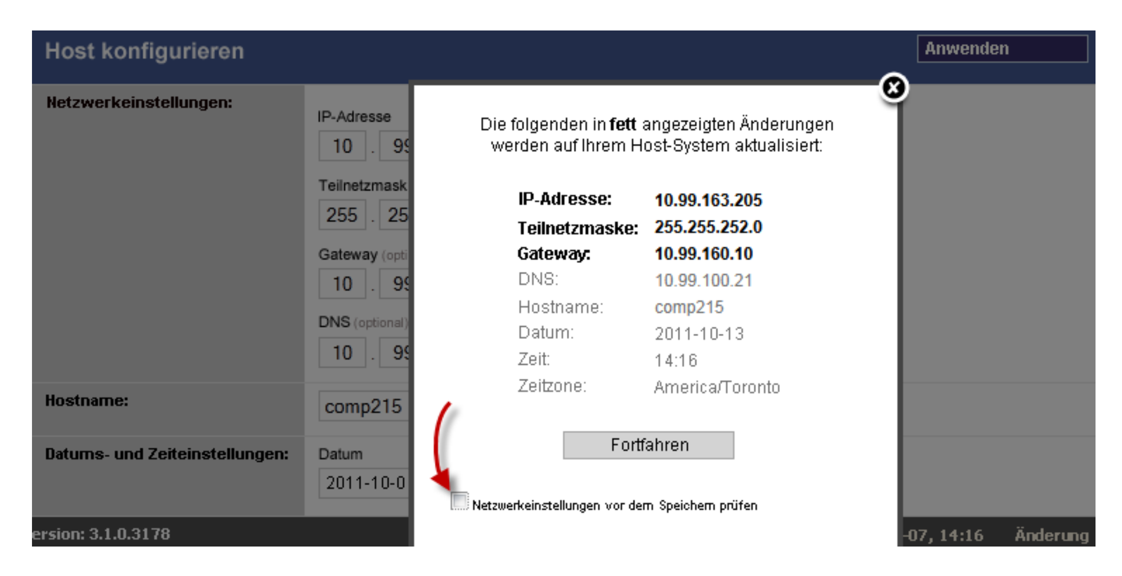
Weitere Informationen hierzu finden Sie unter Appliance-Version 2 – Konfiguration über die Forge-ACC (http://www.novell.com/documentation/platespin_forge_3/getstart/data/bk2otgs.html#bwkc1x9) im *Handbuch „Erste Schritte“*.

5 Starten Sie die Forge Appliance Configuration Console (ACC): Öffnen Sie einen Browser und navigieren Sie zu http://<Forge_IP_Adresse>:10000.

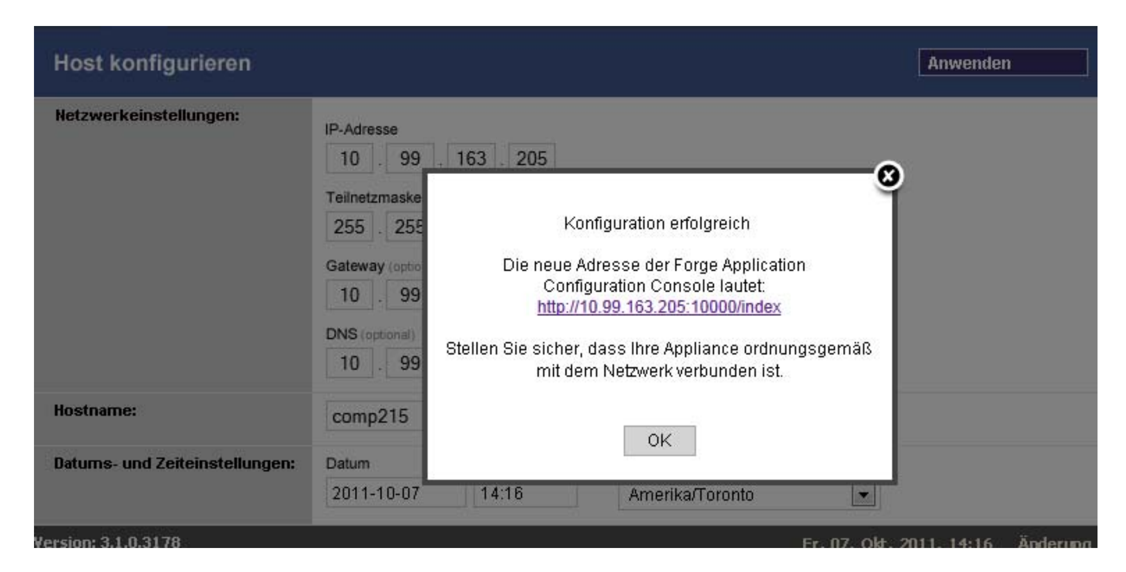
6 Melden Sie sich mit dem `forgeuser`-Konto an und klicken Sie auf *Configure Host* (Host konfigurieren).

7 Geben Sie die neuen Netzwerkeinstellungen ein und klicken Sie auf *Apply* (Anwenden).

8 Vergewissern Sie sich, dass die im Bestätigungsfenster angezeigten neuen Einstellungen korrekt sind. Deaktivieren Sie die Option *Verify network settings before saving* (Netzwerkeinstellungen vor dem Speichern prüfen) und klicken Sie auf *Continue* (Fortfahren).



9 Warten Sie, bis der Konfigurationsvorgang abgeschlossen ist und im Browser das Meldungsfenster „Configuration Successful“ (Konfiguration erfolgreich) geöffnet wird.



Hinweis: Der Link für die neue ACC-Adresse im Meldungsfenster funktioniert erst, nachdem Sie die Appliance physisch getrennt und an das neue Teilnetz angeschlossen haben.

10 Trennen Sie den Computer von der Appliance und schließen Sie die Appliance an das neue Teilnetz an.

Die neue IP-Adresse sollte jetzt gültig sein.

11 Starten Sie die ACC und melden Sie sich mit dem `forgeuser`-Konto an. Klicken Sie auf *Configure Forge VM* (Forge-VM konfigurieren), geben Sie die erforderlichen Parameter an und klicken Sie auf *Apply* (Anwenden).

12 Vergewissern Sie sich, dass die Einstellungen korrekt sind, klicken Sie auf *Continue* (Fortfahren) und warten Sie, bis der Vorgang abgeschlossen ist.

Hinweis: Wenn die Forge-VM für DHCP eingerichtet wurde, führen Sie nach der Standortänderung die folgenden Schritte aus:

1. Ermitteln Sie die neue IP-Adresse der Forge-VM (greifen Sie mithilfe des VMware-Clientprogramms auf die Forge-VM zu und suchen Sie die Adresse in der Windows-Schnittstelle der VM. Weitere Informationen hierzu finden Sie in „Starten des VMware-Clients und Zugriff auf die Forge Management-VM“ auf Seite 42).

2. Verwenden Sie die neue IP-Adresse, um den PlateSpin Forge-Web-Client zu starten, und aktualisieren Sie den Container (klicken Sie auf *Settings* > *Containers* > *(Einstellungen* > *Container) und anschließend auf das Symbol*).

13 Nehmen Sie die angehaltenen Reproduktionen wieder auf.

3.2.2 Standortänderung der Forge-Appliance Version 1

1 Unterbrechen Sie alle Reproduktionszeitpläne. Stellen Sie dabei sicher, dass mindestens eine inkrementelle Reproduktion für jeden Workload ausgeführt wurde:

- **1a** Wählen Sie im Web-Client der PlateSpin Forge-Appliance alle Workloads aus, klicken Sie auf *Unterbrechen* und anschließend auf *Ausführen*.
- **1b** Stellen Sie sicher, dass der Status *Unterbrochen* für alle Workloads angezeigt wird.

2 Fahren Sie die Forge Management-VM herunter. Weitere Informationen hierzu finden Sie unter „Starten und Herunterfahren der Forge Management-VM“ auf Seite 44.

3 Fahren Sie den Appliance-Host herunter:

- **3a** Wechseln Sie an der Forge-Konsole durch Drücken von Alt+F2 zur ESX-Serverkonsole (drücken Sie Alt+F1, um wieder zur Forge-Konsole zu gelangen).
- **3b** Melden Sie sich als „superuser“ an (`root` und das zugehörige Passwort).
- **3c** Geben Sie den folgenden Befehl ein und drücken Sie die Eingabetaste:

```
shutdown -h now
```

- **3d** Schalten Sie die Appliance aus.

4 Stellen Sie die Appliance an einem neuen Ort auf, richten Sie die Hardware ein, nehmen Sie die erforderlichen Kabelanschlüsse vor und schalten Sie dann die Appliance wieder ein.

5 Aktualisieren Sie die Appliance-Netzwerkkonfiguration:

- **5a** Melden Sie sich an der Forge-Konsole als „superuser“ an (`root` und das zugehörige Passwort).

5b Aktualisieren Sie die Einstellungen der *IP-Adresse, Netzmaske und Gateway-IP-Adresse* für den Appliance-Host, wie erforderlich. Sie können DHCP verwenden, aber nur, wenn statische IP-Adressen vergeben werden. Weisen Sie den einzelnen Appliances in einer Umgebung mit mehreren Appliances eindeutige Hostnamen zu, um Hostnamen-Konflikte zu vermeiden.

5c Aktualisieren Sie die Einstellungen der *IP-Adresse, Netzmaske, Gateway-IP-Adresse* und Domänen-Zugehörigkeit für die Forge Management-VM, wie erforderlich.

5d Wählen Sie *OK*, überprüfen Sie die Aktualisierungen und wählen Sie dann erneut *OK*.

6 Aktualisieren Sie die Netzwerkeinstellungen für die unterbrochenen Reproduktionen. Führen Sie im PlateSpin Forge-Web-Client folgende Schritte für jeden unterbrochenen Workload aus:

6a Wechseln Sie in den Abschnitt „Reproduktionseinstellungen" in den Schutzdetails des unterbrochenen Workloads.

6b Aktualisieren Sie den Wert *Reproduktionsnetzwerk* entsprechend der Netzwerkänderung.

6c Speichern Sie die Einstellungen.

7 Nehmen Sie die Reproduktionen wieder auf: Wählen Sie im Web-Client der PlateSpin Forge-Appliance alle Workloads aus, klicken Sie auf *Zeitplan wieder aufnehmen* und anschließend auf *Ausführen*.

3.3 Verwenden externer Speicherlösungen mit PlateSpin Forge

Folgende Abschnitte enthalten Informationen, die Ihnen bei der Einrichtung und Konfiguration eines externen Speichers für die PlateSpin Forge-Appliance helfen.

- Abschnitt 3.3.1, „Verwenden von Forge mit einem SAN-Speicher", auf Seite 39
- Abschnitt 3.3.2, „Hinzufügen einer SAN-LUN zu Forge", auf Seite 41

3.3.1 Verwenden von Forge mit einem SAN-Speicher

Die PlateSpin Forge-Appliance unterstützt vorhandene externe Speicherlösungen wie z. B. SAN-Implementierungen (Storage Area Network). Sowohl Fibre-Channel- als auch iSCSI-Lösungen werden unterstützt. Die SAN-Unterstützung für Fibre-Channel- und iSCSI-HBAs ermöglicht den Anschluss einer Forge-Appliance an einen SAN-Array. Somit können Sie SAN-Array-LUNs (Logical Units) zum Speichern von Workload-Daten verwenden. Die Verwendung der Forge-Appliance mit einem SAN verbessert die Flexibilität, Effizienz und Zuverlässigkeit.

Jedes SAN-Produkt weist individuelle Merkmale und Unterschiede auf, die von Hardwarehersteller zu Hardwarehersteller verschieden sind. Dies zeigt sich insbesondere dann, wenn es um die Art und Weise geht, wie diese Produkte mit der Forge Management-VM verbunden werden und mit dieser interagieren. Aus diesem Grund sprengen spezifische Konfigurationsschritte für jede mögliche Umgebung und jeden Kontext den Rahmen dieses Handbuchs.

Wenden Sie sich für diese Art von Informationen an Ihren Hardware-Anbieter oder Vertriebsbeauftragter für das SAN-Produkt. Viele Hardware-Anbieter verfügen über Dokumentation, in der diese Aufgaben detailliert beschrieben sind. Eine Vielzahl an Informationen finden Sie auf folgenden Websites:

Die Website für VMware-Dokumentation (http://www.vmware.com/support/pubs/).

- Im *Fibre Channel SAN Configuration Guide* wird die Verwendung des ESX-Servers mit Fibre-Channel-SANs erörtert.
- Im *iSCSI SAN Configuration Guide* wird die Verwendung des ESX-Servers mit iSCSI-SANs erörtert.
- Im *VMware I/O Compatibility Guide* werden die aktuell genehmigten HBAs, HBA-Treiber und Treiberversionen aufgeführt.
- Im *VMware Storage/SAN Compatibility Guide* werden die aktuell genehmigten Speicher-Arrays aufgeführt.
- Die *VMware-Versionshinweise* bieten Informationen zu bekannten Problemen und Ausweichlösungen.
- Die *VMware Knowledge Bases* enthalten Informationen zu bekannten Problemen und Ausweichlösungen.

Folgende Hersteller bieten Speicherprodukte, die von VMware getestet wurden:

- 3PAR (http://www.3par.com)
- Bull (http://www.bull.com) (nur FC)
- Compellent (http://www.compellent.com)
- Dell (http://www.dell.com)
- EMC (http://www.emc.com)
- EqualLogic (http://www.equallogic.com) (nur iSCSI)
- Fujitsu (http://www.fujitsu.com) und Fujitsu Siemens (http://www.fujitsu-siemens.com)
- HP (http://www.hp.com)
- Hitachi (http://www.hitachi.com) und Hitachi Data Systems (http://www.hds.com) (nur FC)
- IBM (http://www.ibm.com)
- NEC (http://www.nec.com) (nur FC)
- Network Appliance (NetApp) (http://www.netapp.com)
- Nihon Unisys (http://www.unisys.com) (nur FC)
- Pillar Data (http://www.pillardata.com) (nur FC)
- Sun Microsystems (http://www.sun.com)
- Xiotech (http://www.xiotech.com) (nur FC)

Weitere Informationen über iSCSI finden Sie außerdem auf der Website der Storage Networking Industry Association unter http://www.snia.org/tech_activities/ip_storage/iscsi/.

3.3.2 Hinzufügen einer SAN-LUN zu Forge

PlateSpin Forge unterstützt die SAN-Speicherung (Storage Area Network). Damit Forge auf ein vorhandenes SAN zugreifen kann, muss jedoch zuerst eine SAN-LUN (Logical Unit) zum Forge-ESX-Server hinzugefügt werden.

1 Richten Sie Ihr SAN-System ein und konfigurieren Sie es.

2 Greifen Sie auf den Appliance-Host zu (siehe „Herunterladen des VMware-Clientprogramms“ auf Seite 42).
3 Klicken Sie im VMware-Client im Inventarbereich auf den Stammknoten (den obersten Knoten) und wählen Sie die Registerkarte *Konfiguration*.
4 Klicken Sie auf den Hyperlink *Add Storage* (Speicher hinzufügen) oben rechts.
5 Klicken Sie im Assistenten zum Hinzufügen von Speicher auf *Next* (Weiter), bis Sie aufgefordert werden, Datenablageinformationen anzugeben.
6 Geben Sie einen Datenablagenamen ein und klicken Sie in den daraufhin angezeigten Assistentenseiten auf *Next* (Weiter). Klicken Sie auf *Fertig stellen*, wenn der Assistent abgeschlossen ist.
7 Klicken Sie unter *Hardware* auf *Storage* (Speicher), um die Forge-Datenablagen anzuzeigen. Die neu hinzugefügte SAN-LUN sollte im Fenster angezeigt werden.
8 Beenden Sie das VMware-Clientprogramm.

Im Web-Client der PlateSpin Forge-Appliance wird die neue Datenablage erst nach der nächsten Reproduktion und Aktualisierung des Anwendungshosts angezeigt. Sie können eine Aktualisierung erzwingen, indem Sie *Settings* > *Containers* (Einstellungen, Container) wählen und auf nahe dem Appliance-Hostnamen klicken.

3.4 Wartung der PlateSpin Forge-Appliance

In diesem Kapitel werden die Aufgaben zur Wartung der PlateSpin Forge-Appliance beschrieben.

- Abschnitt 3.4.1, „Forge Management-VM im Appliance-Host - Zugriff und Verwendung“, auf Seite 41

3.4.1 Forge Management-VM im Appliance-Host - Zugriff und Verwendung

Gelegentlich müssen Sie auf die Forge Management-VM zugreifen und Wartungsaufgaben durchführen, wie in diesem Handbuch beschrieben, oder Sie erhalten vom PlateSpin-Support die Empfehlung zur Durchführung von Wartungsarbeiten.

Verwenden Sie dieVMware-Clientsoftware, um auf die Forge Management-VM, deren Betriebssystemschnittstelle und die VM-Einstellungen zuzugreifen.

Hinweis: Die VMware-Clientsoftware ist bei ESX Version 3.5 (Forge-Appliance Version 1) und ESX Version 4.1 (Forge-Appliance Version 2) unterschiedlich.

- ESX 3.5 benötigt den VMware Virtual Infrastructure Client (VIC)
- ESX 4.1 benötigt den VMware vSphere-Client

Der Einfachheit halber werden diese Programme manchmal als *VMware-Client* bezeichnet. Darüber hinaus werden die Begriffe *Virtual Infrastructure Client (VIC)* und *vSphere-Client* möglicherweise synonym verwendet.

- „Herunterladen des VMware-Clientprogramms“ auf Seite 42
- „Starten des VMware-Clients und Zugriff auf die Forge Management-VM“ auf Seite 42
- „Starten und Herunterfahren der Forge Management-VM“ auf Seite 44

- „Verwalten von Forge-Snapshots auf dem Appliance-Host“ auf Seite 44
- „Manuelles Importieren von VMs in die Datenablage des Appliance-Hosts“ auf Seite 45
- „Richtlinien zur Anwendung von Sicherheitsaktualisierungen auf die PlateSpin Forge Management-VM“ auf Seite 45

Herunterladen des VMware-Clientprogramms

Laden Sie die Clientsoftware vom Appliance-Host herunter und installieren Sie sie auf einer Windows-Arbeitsstation außerhalb von der PlateSpin Forge-Appliance.

1 Laden Sie die Clientsoftware herunter:

- (Bedingt: für Forge-Appliance Version 2 mit VMware ESX 4.1) Laden Sie das Programm VMware vSphere-Client (http://vsphereclient.vmware.com/vsphereclient/3/4/5/0/4/3/VMware-viclient-all-4.1.0-345043.exe)herunter.

  ODER

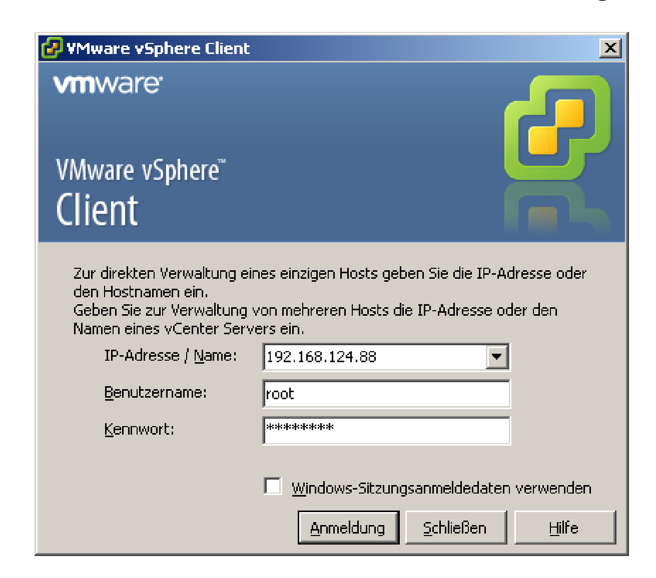
- (Bedingt: für Forge-Appliance Version 1 mit VMware ESX 3.5) Öffnen Sie einen Webbrowser und wechseln Sie zur Startseite des Appliance-Hosts (VMware ESX). Verwenden Sie dazu die IP-Adresse des Appliance-Hosts. Ignorieren Sie die Warnung bezüglich des Sicherheitszertifikats. Klicken Sie auf der Begrüßungsseite des VMware ESX-Servers auf *Download Virtual Infrastructure Client* (Virtual Infrastructure Client herunterladen) und laden Sie das Installationsprogramm herunter.

2 Starten Sie das heruntergeladene Installationsprogramm und befolgen Sie die Anweisungen zum Installieren der Software.

Starten des VMware-Clients und Zugriff auf die Forge Management-VM

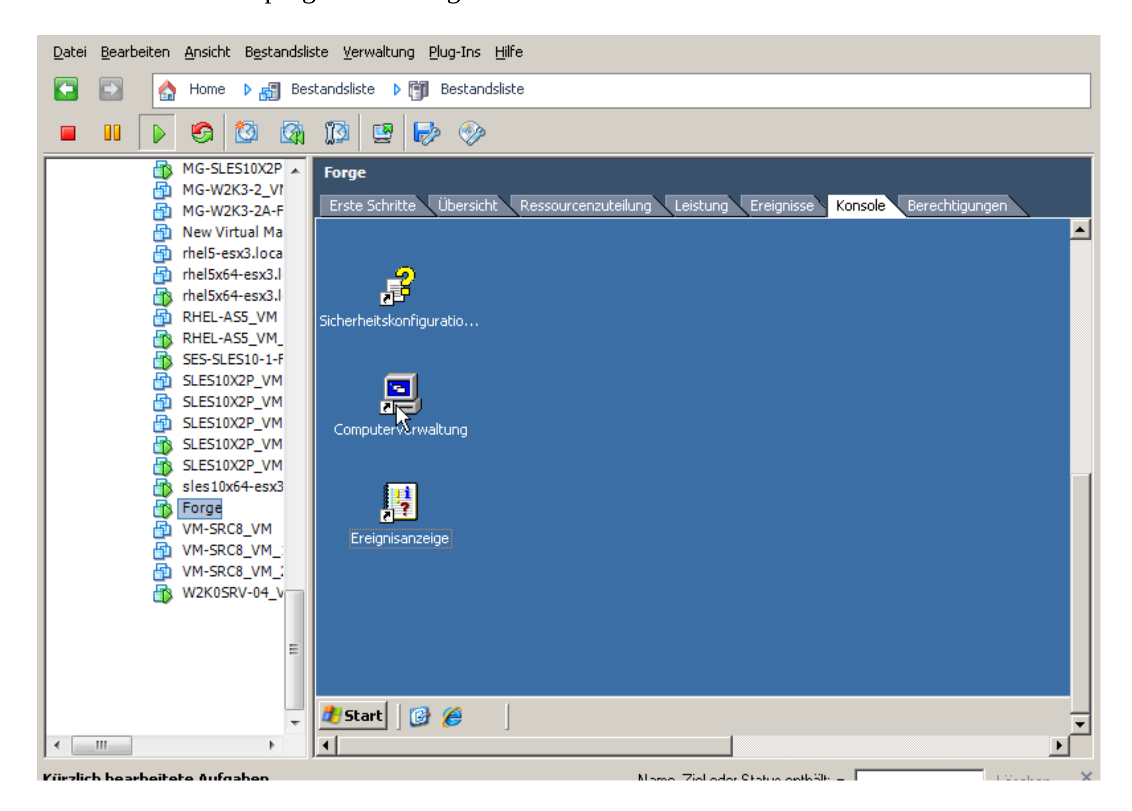
1 Klicken Sie auf *Start* > *Programme* > *VMWare* > *VMware vSphere* | *Virtual InfrastrucureClient*.

Das Anmeldefenster des VMware-Clients wird angezeigt.



2 Geben Sie Ihren Berechtigungsnachweis der Root-Ebene ein und melden Sie sich an. Ignorieren Sie eventuell angezeigte Zertifikatswarnungen.

Das VMware-Clientprogramm wird geöffnet.



3 Wählen Sie im Inventarbereich auf der linken Seite das Element *PlateSpin Forge Management VM* aus. Klicken Sie im rechten Bereich auf die Registerkarte *Console* (Konsole).

Der Konsolenbereich des Clients zeigt die Windows-Schnittstelle der Forge Management-VM an.

Arbeiten Sie über die Konsole genauso mit der Management-VM, wie Sie auf einem physischen Computer mit Windows arbeiten würden.

Klicken Sie zum Entsperren der Management-VM in die Konsole und drücken Sie „Strg+Alt+Einfg“.

Um den Cursor für die Arbeit außerhalb des VMware-Clientprogramms freizugeben, drücken Sie „Strg+Alt“.

Starten und Herunterfahren der Forge Management-VM

Gelegentlich kann es erforderlich sein, die Forge Management-VM herunterzufahren und neu zu starten, z. B. wenn sich der Standort der Appliance ändert.

1 Verwenden Sie den VMware Client für den Zugriff auf den Forge Management-VM-Host. Weitere Informationen hierzu finden Sie unter „Herunterladen des VMware-Clientprogramms“ auf Seite 42.

2 Verwenden Sie das Windows-Standardverfahren zum Herunterfahren der VM (*Start* > *Herunterfahren*).

So starten Sie die Management-VM neu:

1. Klicken Sie im Inventarbereich auf der linken Seite mit der rechten Maustaste auf das Element *PlateSpin Forge Management VM* und wählen Sie *Power on* (Einschalten).

Verwalten von Forge-Snapshots auf dem Appliance-Host

Gelegentlich kann es erforderlich sein, einen Snapshot der Management-VM zu erstellen, z. B. beim Aktualisieren der Forge-Software oder beim Durchführen von Aufgaben zur Fehlerbehebung. Möglicherweise müssen Sie auch Snapshots (Wiederherstellungspunkte) entfernen, um Speicherplatz frei zu machen.

1. Verwenden Sie den VMware-Client für den Zugriff auf den Appliance-Host. Weitere Informationen hierzu finden Sie unter „Herunterladen des VMware-Clientprogramms“ auf Seite 42.
2. Klicken Sie im Inventarbereich auf der linken Seite mit der rechten Maustaste auf das Element *PlateSpin Forge Management VM* und wählen Sie *Snapshot* > *Take Snapshot* (Snapshot, Snapshot erstellen).
3. Geben Sie einen Namen und eine Beschreibung für den Snapshot ein und klicken Sie anschließend auf *OK*.

So versetzen Sie die Management-VM in einen früheren Zustand zurück:

1. Klicken Sie im Inventarbereich auf der linken Seite mit der rechten Maustaste auf das Element *PlateSpin Forge Management VM* und wählen Sie *Snapshot* > *Snapshot Manager*.
2. Wählen Sie in der Baumdarstellung der VM-Zustände einen Snapshot aus und klicken Sie anschließend auf *Go to* (Wechseln zu).

So entfernen Sie Snapshots, die Wiederherstellungspunkte darstellen:

1. Klicken Sie im Inventarbereich auf der linken Seite mit der rechten Maustaste auf das Element *PlateSpin Forge Management VM* und wählen Sie *Snapshot* > *Snapshot Manager*.
2. Wählen Sie in der Baumdarstellung der VM-Zustände einen Snapshot aus und klicken Sie anschließend auf *Remove* (Entfernen).

Manuelles Importieren von VMs in die Datenablage des Appliance-Hosts

Verwenden Sie diese Prozedur, um eine VM in die Datenablage des Appliance-Hosts zu importieren. Sie können diese Option verwenden, wenn Sie Ihren Wiederherstellungs-Workload unterschiedlich erstellen möchten (siehe „Anfängliche Reproduktionsmethode (Vollständig und Inkrementell)“ auf Seite 86).

1. Erstellen Sie am Produktionsstandort eine VM (ESX 3.5 und höher) aus Ihrem Produktions-Workload (z. B. mit PlateSpin Migrate) und kopieren Sie die VM-Dateien von der Datenablage des ESX-Host auf einen Wechseldatenträger, wie z. B. eine externe Festplatte oder einen USB-Stick. Verwenden Sie den „Datenspeicherbrowser“ der Clientsoftware zum Auffinden der Dateien.
2. Schließen Sie am Disaster Recovery-Standort den Wechseldatenträger an einer Arbeitsstation an, die über Netzwerkzugriff auf Forge verfügt und auf der das VMware-Clientprogramm installiert ist. Weitere Informationen hierzu finden Sie in „Herunterladen des VMware-Clientprogramms“ auf Seite 42.

3. Verwenden Sie den „Datenspeicherbrowser“ des VMware-Clients, um auf die Forge-Datenablage (*Storage1*) zuzugreifen, und laden Sie die VM-Dateien vom Wechseldatenträger hoch. Verwenden Sie die hochgeladene VM, um sie mit dem Appliance-Host zu registrieren (klicken Sie mit der rechten Maustaste auf *Zur Bestandsliste hinzufügen*).
4. Aktualisieren Sie das PlateSpin Forge-Inventar (klicken Sie im PlateSpin Forge-Web-Client auf *Einstellungen* > *Container* und anschließend auf das Symbol neben dem Appliance-Host).

Richtlinien zur Anwendung von Sicherheitsaktualisierungen auf die PlateSpin Forge Management-VM

Dieser Abschnitt bietet allgemeine Richtlinien zur Anwendung von Sicherheitspatches auf die Forge Management-VM.

1. Rufen Sie während eines Wartungsfensters die Forge Management-VM über das VMware-Clientprogramm auf. Weitere Informationen hierzu finden Sie unter „Herunterladen des VMware-Clientprogramms“ auf Seite 42.
2. Suchen Sie von der Windows-Benutzeroberfläche der Forge Management-VM aus nach Sicherheitsaktualisierungen von Microsoft.
3. Versetzen Sie PlateSpin Forge mithilfe des PlateSpin Forge-Web-Clients in den Wartungsmodus, indem Sie alle Reproduktionszeitpläne anhalten und warten, bis alle laufenden Reproduktionen abgeschlossen sind.
4. Erstellen Sie einen Snapshot der Forge Management-VM. Weitere Informationen hierzu finden Sie unter „Verwalten von Forge-Snapshots auf dem Appliance-Host“ auf Seite 44.
5. Laden Sie die erforderlichen Sicherheitspatches herunter und installieren Sie sie. Wenn die Installation abgeschlossen ist, starten Sie die Forge Management-VM neu.
6. Nehmen Sie die in Schritt 3 angehaltenen Reproduktionen mithilfe des PlateSpin Forge-Web-Clients wieder auf und vergewissern Sie sich, dass die Reproduktionen ordnungsgemäß funktionieren.
7. Entfernen Sie den in Schritt 4 erstellten Snapshot der Forge Management-VM. Weitere Informationen hierzu finden Sie unter „Verwalten von Forge-Snapshots auf dem Appliance-Host“ auf Seite 44.

3.5 Aufrüsten von PlateSpin Forge

Dieser Abschnitt enthält Informationen zur Aufrüstung der PlateSpin Forge-Appliance.

3.5.1 Vor Beginn der Aufrüstung

Stellen Sie vor der Aufrüstung sicher, dass Sie folgende Komponenten zur Hand haben:

- Die Forge-Installations- und Einrichtungsprogrammdatei.

- Die IP-Adressen und Berechtigungsnachweise für:
  - Die Forge-Appliance (wird für die Forge-Web-Client-Schnittstelle und die Forge Management-VM verwendet)
  - Den Forge-Appliance-Host (VMware ESX-Server)
- Das VMware-Clientprogramm. Weitere Informationen hierzu finden Sie in „Herunterladen des VMware-Clientprogramms“ auf Seite 42.

3.5.2 Zusammenfassung der Aufrüstungsaufgaben

Zum Aufrüsten der Forge-Appliance müssen Sie folgenden Aufgaben in der angegebenen Reihenfolge durchführen:

1. Stellen Sie sicher, dass gerade keine Reproduktionen ausgeführt werden oder für den Zeitraum während der Aufrüstung geplant sind.
2. Speichern Sie den aktuellen Zustand der Management-VM, indem Sie einen Snapshot erstellen.
3. Aktualisieren Sie die Forge Management-VM mit der neuesten Microsoft .NET Framework-Software und allen Sicherheitspatches.
4. Kopieren Sie die erforderliche Einrichtungsprogrammdatei und führen Sie sie lokal in der Forge Management-VM aus.
5. Vergewissern Sie sich, dass die Appliance nach dem Aufrüsten ordnungsgemäß funktioniert.

3.5.3 Forge-Aufrüstungsverfahren

In dieser Phase müssen alle geplanten Reproduktionen geschützter Workloads angehalten werden. Außerdem muss gewartet werden, bis laufende Reproduktionen abgeschlossen sind.

1 Halten Sie geplante Reproduktionen über den PlateSpin Forge-Web-Client an. Warten Sie, bis eventuell laufende Reproduktionen abgeschlossen sind. Stellen Sie sicher, dass der Reproduktionsstatus geschützter Workloads in der entsprechende Spalte mit *Im Leerlauf* angezeigt wird.

Weitere Informationen hierzu finden Sie in „Starten des PlateSpin Forge-Web-Clients“ auf Seite 49.

2 Schalten Sie die Forge Management-VM aus. Weitere Informationen hierzu finden Sie unter „Starten und Herunterfahren der Forge Management-VM“ auf Seite 44.

3 Sichern Sie die Forge Management-VM durch Erstellen eines Snapshots. Weitere Informationen hierzu finden Sie unter „Verwalten von Forge-Snapshots auf dem Appliance-Host“ auf Seite 44.

4 Deaktivieren Sie bei Forge 1.x-Appliances den Modus „Independent“ (Unabhängig) für die VM-Festplatte 2:

4a Klicken Sie im Inventarbereich auf der linken Seite mit der rechten Maustaste auf die Forge-Management VM und wählen Sie *Edit Settings* (Einstellungen bearbeiten).

Das Fenster mit den Eigenschaften der virtuellen Maschine wird angezeigt.

4b Klicken Sie auf der Registerkarte *Hardware* auf *Hard Disk 2* (Festplatte 2).

4c Deaktivieren Sie auf der rechten Seite das Kontrollkästchen *Unabhängig*.

5 Schalten Sie die Forge Management-VM ein, greifen Sie über das VMware-Clientprogramm darauf zu und führen Sie folgende Schritte aus:

5a Installieren Sie die neueste Microsoft .NET Framework-Software. Forge 3 erfordert mindestens Microsoft .NET Framework 3.5, SP1 (http://www.microsoft.com/downloads/details.aspx?FamilyId=AB99342F-5D1A-413D-8319-81DA479AB0D7).

5b Aktualisieren Sie Windows. Wenden Sie dabei alle verfügbaren Sicherheitsaktualisierungen an.

5c Starten Sie die Forge Management-VM neu.

6 Führen Sie die Programmdatei zur Forge-Installation und -Einrichtung innerhalb der Forge Management-VM aus und befolgen Sie die Anweisungen auf dem Bildschirm.

Hinweis: In einigen Situationen kann das Installationsprogramm möglicherweise Daten, die es während des Aufrüstprozesses exportiert hat, nicht automatisch wieder importieren. Verwenden Sie in diesem Fall das Dienstprogramm `PlateSpin.ImportExport.exe`, um diese Daten vom Verzeichnis `\Dokumente und Einstellungen\<Benutzerprofil>\Anwendungsdaten\PlateSpin` Ihres Server-Hosts wiederherzustellen. Weitere Informationen hierzu finden Sie im KB-Artikel 7921084 (http://www.novell.com/support/viewContent.do?externalId=7921084).

---

7 Nehmen Sie alle angehaltenen Reproduktionen über den PlateSpin Forge-Web-Client wieder auf.

8 Entfernen Sie mithilfe des VMware-Clientprogramms den Snapshot, den Sie in Schritt 3 erstellt haben.

Wichtig: Treiber, die für ein Failback in die Treiberdatenbank von PlateSpin Forge heraufgeladen wurden, werden nicht beibehalten. Solche Treiber müssen nach der Aufrüstung erneut heraufgeladen werden.

---

4 Aufgestellt und in Betrieb

In diesem Kapitel werden die wichtigsten Funktionen von PlateSpin Forge und seiner Schnittstelle beschrieben.

4.1 Starten des PlateSpin Forge-Web-Clients

Die meisten Aktionen mit PlateSpin Forge führen Sie über den browserbasierten PlateSpin Forge-Web-Client durch.

Die folgenden Browser werden unterstützt:

- Microsoft Internet Explorer 7 und höher
- Mozilla Firefox (unter Windows) 3.6 und höher

JavaScript (Active Scripting) muss in Ihrem Browser aktiviert sein:

- **Internet Explorer:** Klicken Sie auf *Extras* > *Internetoptionen* > *Sicherheit* > *Zone „Internet“* > *Stufe anpassen* und wählen Sie anschließend die Option *Aktivieren* für die Active Scripting-Funktion aus.
- **Firefox:** Klicken Sie auf *Extras* > *Einstellungen* > *Inhalt* und wählen Sie anschließend die Option *JavaScript aktivieren* aus.

Informationen zur Verwendung des PlateSpin Forge Web-Clients und der integrierten Hilfe in einer der unterstützten Sprachen finden Sie unter Abschnitt 2.4.2, „Einrichtung der Sprache bei internationalen Versionen von PlateSpin Forge“, auf Seite 28.

So starten Sie den PlateSpin Forge-Web-Client:

1. Öffnen Sie einen Webbrowser und wechseln Sie zu folgender Adresse:

   `http://`*<Hostname | IP-Adresse>*`/Forge`

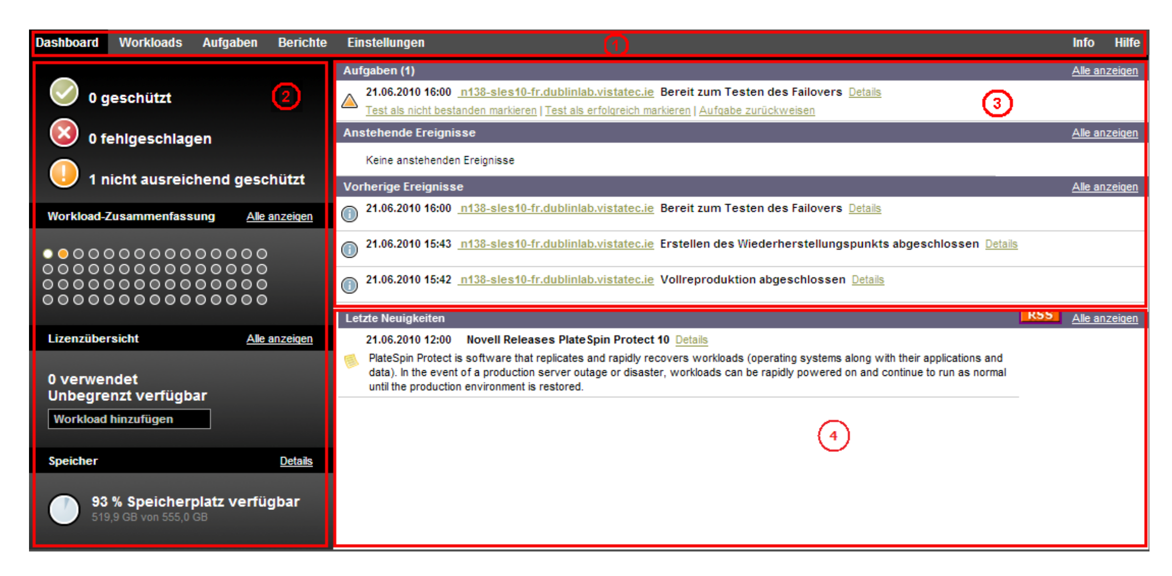
   Ersetzen Sie *<Hostname | IP-Adresse>* durch den Hostnamen bzw. die IP-Adresse Ihrer Forge-VM.

   Wenn SSL aktiviert ist, verwenden Sie `https` in der URL.

4.2 Elemente des PlateSpin Forge-Web-Clients

Die Standardschnittstelle des PlateSpin Forge-Web-Clients ist die Seite „Dashboard“, die Elemente zum Navigieren zu verschiedenen Funktionsbereichen der Schnittstelle und zum Durchführen von Workload-Schutz- und Wiederherstellungsaufgaben bereitstellt.

Abbildung 4-1 *Die Standard-Dashboard-Seite des PlateSpin Forge-Web-Clients*



Die Dashboard-Seite besteht aus den folgenden Elementen:

- **Navigationsleiste:** Auf den meisten Seiten des PlateSpin Forge-Web-Clients enthalten.
- **Teilfenster mit visueller Zusammenfassung:** Bietet einen umfassenden Überblick über den Gesamtstatus des Workload-Inventars von PlateSpin Forge.
- **Teilfenster mit Aufgaben und Ereignissen:** Bietet Informationen über Ereignisse und Aufgaben, die einen Eingriff des Benutzers erfordern.
- **Teilfenster „Letzte Neuigkeiten“:** Bietet mittels RSS Informationen zum Produkt und zu zugehörigen Aktualisierungen. Wenn Sie den RSS-Feed zu PlateSpin Forge abonnieren möchten, klicken Sie auf *RSS*.

Die folgenden Abschnitte enthalten weitere Informationen.

- Abschnitt 4.2.1, „Navigationsleiste“, auf Seite 51
- Abschnitt 4.2.2, „Teilfenster mit visueller Zusammenfassung“, auf Seite 51
- Abschnitt 4.2.3, „Teilfenster mit Aufgaben und Ereignissen“, auf Seite 52

4.2.1 Navigationsleiste

Die Navigationsleiste enthält folgende Links:

- **Dashboard:** Zeigt die Standardseite „Dashboard“ an.
- **Workloads:** Zeigt die Seite „Workloads“ an. Weitere Informationen hierzu finden Sie unter „Workloads und Workload-Befehle“ auf Seite 52.
- **Aufgaben:** Zeigt die Seite „Aufgaben“ mit den Elementen an, die einen Benutzereingriff erfordern.
- **Berichte:** Zeigt die Seite „Berichte“ an. Weitere Informationen hierzu finden Sie unter „Generieren von Workload- und Workload-Schutz-Berichten“ auf Seite 57.
- **Einstellungen:** Zeigt die Seite „Einstellungen“ an, die Zugriff auf die folgenden Konfigurationsoptionen bietet:
  - **Schutzebenen:** Weitere Informationen hierzu finden Sie unter „Schutzebenen“ auf Seite 85.
  - **Berechtigungen:** Weitere Informationen hierzu finden Sie in „Einrichten der Benutzerautorisierung und -authentifizierung“ auf Seite 18.
  - **Email/SMTP:** Weitere Informationen hierzu finden Sie in „Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“ auf Seite 26.
  - **Lizenzen/Lizenzbezeichnungen:** Weitere Informationen hierzu finden Sie in „Produktlizenzierung“ auf Seite 17.

4.2.2 Teilfenster mit visueller Zusammenfassung

Das Teilfenster mit der visuellen Zusammenfassung bietet eine effiziente Ansicht aller lizenzierten Workloads sowie der Menge an verfügbarem Speicher auf der Appliance.

Inventarisierte Workloads werden in drei Kategorien dargestellt:

- **Geschützt:** Gibt die Anzahl der aktiv geschützten Workloads an.
- **Fehlgeschlagen:** Gibt die Anzahl der geschützten Workloads an, die das System gemäß der Schutzebene dieses Workloads als fehlgeschlagen ausgegeben hat.
- **Nicht ausreichend geschützt:** Gibt die Anzahl der geschützten Workloads an, die einen Eingriff des Benutzers erfordern.

Der Bereich in der Mitte des linken Teilfensters stellt eine grafische Zusammenfassung der Seite „Workloads“ dar. Er verwendet Punktsymbole, um die verschiedenen Statusformen der Workloads anzuzeigen:

Tabelle 4-1 *Punktsymbol-Darstellung des Workload-Status*

Ungeschützt	*Nicht ausreichend geschützt*
Ungeschützt – Fehler	*Fehlgeschlagen*
Geschützt	*Abgelaufen*
Nicht verwendet	

Die Symbole werden in alphabetischer Reihenfolge gemäß dem Workload-Namen angezeigt. Richten Sie den Mauszeiger auf ein Punktsymbol, um den Namen des Workloads anzuzeigen, oder klicken Sie darauf, um die zugehörige Seite mit den Workload-Details zu öffnen.

Speicher bietet Informationen über den für PlateSpin Forge verfügbaren Speicherplatz.

4.2.3 Teilfenster mit Aufgaben und Ereignissen

Das Teilfenster mit den Aufgaben und Ereignissen zeigt die letzten Aufgaben und vorherigen Ereignisse sowie die nächsten anstehenden Ereignisse an.

Ereignisse werden protokolliert, wenn sie für das System oder den Workload relevant sind. Ereignisse sind beispielsweise das Hinzufügen eines neuen geschützten Workloads, das Starten oder Fehlschlagen der Reproduktion eines Workloads oder die Erkennung eines Fehlers eines geschützten Workloads. Einige Ereignisse generieren automatische Email-Benachrichtigungen, wenn SMTP konfiguriert ist. Weitere Informationen hierzu finden Sie in „Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“ auf Seite 26.

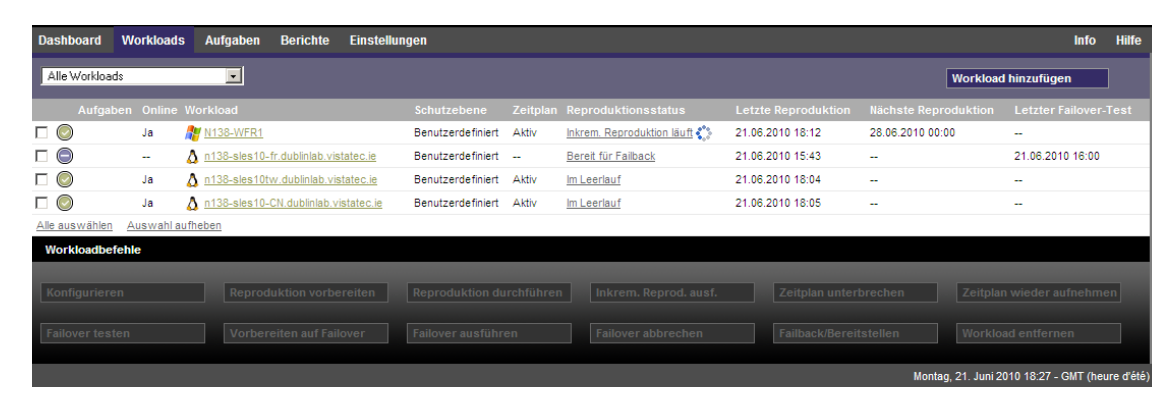
Aufgaben sind spezielle Befehle, die mit Ereignissen verbunden sind, die den Eingriff des Benutzers erfordern. Beispiel: Nach Abschluss des Befehls „Failover testen“ generiert das System ein Ereignis, das mit zwei Aufgaben verbunden ist: `Test als erfolgreich markieren` und `Test als nicht bestanden markieren`. Wenn Sie auf eine der Aufgaben klicken, wird der Failover-Test abgebrochen und es wird ein entsprechendes Ereignis in das Protokoll geschrieben. Ein weiteres Beispiel ist das Ereignis `FullReplicationFailed`, das zusammen mit einer `StartFull`-Aufgabe gezeigt wird. Sie finden eine vollständige Liste der aktuellen Aufgaben auf der Registerkarte *Aufgaben*.

Im Teilfenster „Aufgaben und Ereignisse“ auf dem Dashboard werden für jede Kategorie maximal drei Einträge angezeigt. Wenn alle Aufgaben oder vergangene und anstehende Ereignisse angezeigt werden sollen, klicken Sie im entsprechenden Abschnitt auf *Alle anzeigen*.

4.3 Workloads und Workload-Befehle

Die Seite „Workloads“ enthält eine Tabelle mit einer Zeile pro inventarisiertem Workload. Klicken Sie auf einen Workload-Namen, um die zugehörige Seite „Workload-Details“ anzuzeigen, in der Sie für den Workload und seinen Status relevante Konfigurationen ansehen und bearbeiten können.

***Abbildung 4-2** Die Seite „Workloads“*

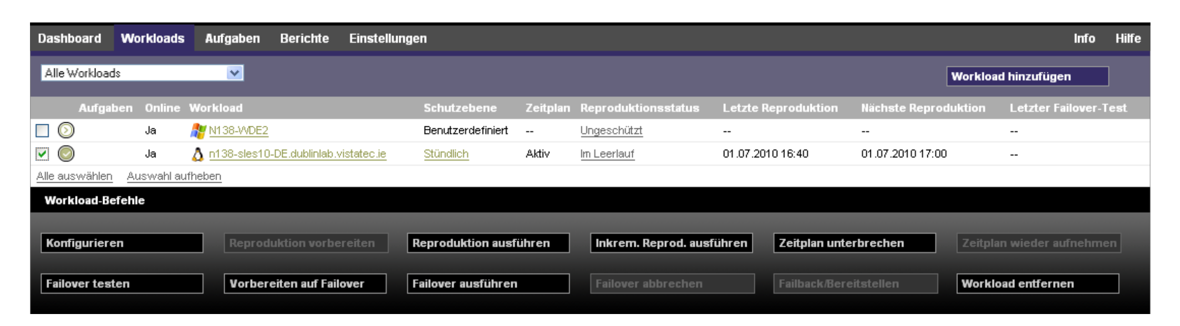


Hinweis: Alle Zeitstempel entsprechen der Zeitzone der Forge-VM. Diese kann sich von der Zeitzone des geschützten Workloads oder der Zeitzone des Hosts, auf dem Sie den PlateSpin Forge-Web-Client ausführen, unterscheiden. Unten rechts im Client-Fenster werden das Serverdatum und die Serveruhrzeit angezeigt.

4.3.1 Workload-Schutz- und Wiederherstellungsbefehle

Befehle spiegeln den Workflow des Workload-Schutzes und der Wiederherstellung wider. Wählen Sie zur Ausführung eines Befehls für einen Workload das entsprechende Kontrollkästchen auf der linken Seite aus. Anwendbare Befehle hängen vom aktuellen Status eines Workloads ab.

Abbildung 4-3 *Workload-Befehle*



In der folgenden Tabelle finden Sie eine Übersicht über die Workload-Befehle sowie deren Beschreibung.

Tabelle 4-2 *Workload-Schutz- und Wiederherstellungsbefehle*

Workload-Befehl	Beschreibung
Konfigurieren	Startet die Konfiguration des Workload-Schutzes mit Parametern, die auf einen inventarisierten Workload anwendbar sind.
Reproduktion vorbereiten	Installiert erforderliche Datenübertragungs-Software auf dem Ursprungscomputer und erstellt eine Failover-VM als Vorbereitung der Workload-Reproduktion.
Reproduktion durchführen	Beginnt die Reproduktion des Ursprungs-Workloads gemäß den angegebenen Parametern.
Inkremental ausführen	Führt einen Transfer von geänderten Daten vom Ursprung zum Ziel außerhalb der im Zeitplan für den Workload-Schutz festgelegten Zeiten durch.
Zeitplan unterbrechen	Unterbricht den Schutz und Datentransfer vom geschützten Workload.
Zeitplan wieder aufnehmen	Nimmt den Schutz gemäß den gespeicherten Schutzeinstellungen wieder auf.
Failover testen	Versetzt den Wiederherstellungs-Workload zu Testzwecken in einer isolierten Umgebung innerhalb des Containers in den Online-Modus.
Vorbereiten auf Failover	Bootet den Wiederherstellungs-Workload in Vorbereitung eines Failover-Vorgangs.

Workload-Befehl	Beschreibung
Failover ausführen	Bootet und konfiguriert den Wiederherstellungs-Workload, der die Geschäftsdienste eines fehlgeschlagenen Workloads übernimmt.
Failover abbrechen	Bricht den Failover-Vorgang ab.
Failback durchführen/ Bereitstellen	Überführt den Wiederherstellungs-Workload nach einem Failover-Vorgang per Failback wieder in die ursprüngliche oder in eine neue Infrastruktur (virtuell oder physisch).
Workload entfernen	Entfernt einen Workload aus dem Inventar.

4.4 Verwenden von Workload-Schutz-Funktionen über die PlateSpin Forge-Web-Services-API

Mithilfe der `protection.webservices`-API können Sie Workload-Schutz-Funktionen programmatisch von Ihren Anwendungen aus verwenden. Sie können alle Programmier- oder Skriptsprachen verwenden, die Web-Services unterstützen.

`http://`<*Hostname* | *IP-Adresse*>`/protection.webservices`

Ersetzen Sie <*Hostname* | *IP-Adresse*> durch den Hostnamen bzw. die IP-Adresse Ihrer Forge-VM.

Wenn Sie Skripte für häufige Workload-Schutz-Vorgänge schreiben möchten, verwenden Sie die in Python geschriebenen Referenzbeispiele als Orientierungshilfe. Eine Microsoft Silverlight-Anwendung wird zusammen mit dem Quellcode ebenfalls zu Referenzzwecken bereitgestellt.

4.5 Verwaltung mehrerer Instanzen von PlateSpin Forge

PlateSpin Forge enthält eine webbasierte Client-Anwendung, die PlateSpin Forge-Verwaltungskonsole, die zentralen Zugriff auf mehrere Instanzen von PlateSpin Forge bietet.

In einem Rechenzentrum mit mehreren Instanzen von PlateSpin Forge können Sie eine der Instanzen als Manager festlegen und die Verwaltungskonsole von dort aus ausführen. Weitere Instanzen werden unter dem Manager hinzugefügt, sodass ein zentraler Punkt für die Steuerung und Interaktion zur Verfügung steht.

4.5.1 Verwenden der PlateSpin Forge-Verwaltungskonsole

1 Öffnen Sie einen Webbrowser auf einem Computer, der Zugriff auf die PlateSpin Forge-Instanzen hat, und navigieren Sie zu folgender URL:

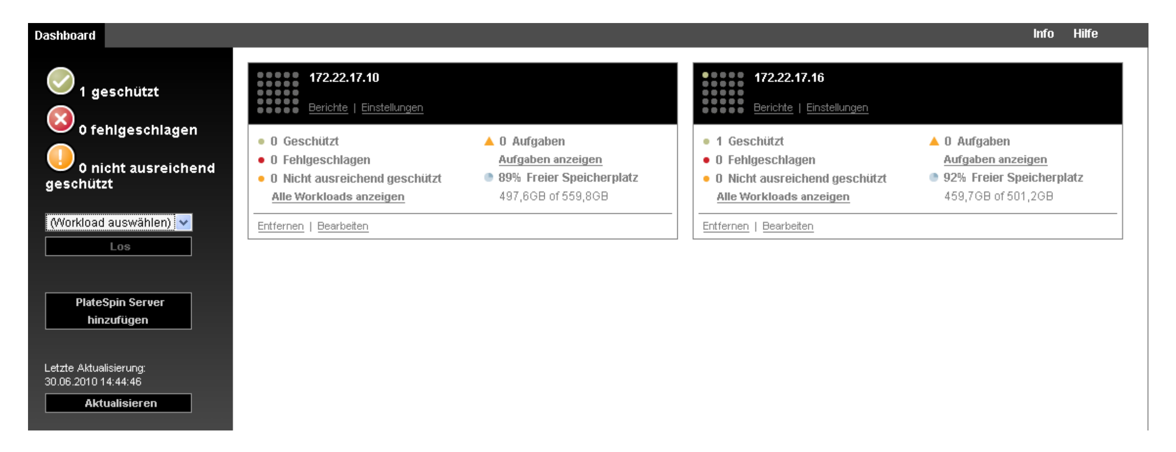
   `http://`<*IP-Adresse* | *Hostname*>`/Konsole`

Ersetzen Sie <*IP-Adresse* | *Hostname*> durch die IP-Adresse oder den Hostnamen der Forge-VM, die als Manager festgelegt wurde.

2 Melden Sie sich mit Ihrem Benutzernamen und Passwort an.

Die Standardseite „Dashboard“ der Konsole wird angezeigt.

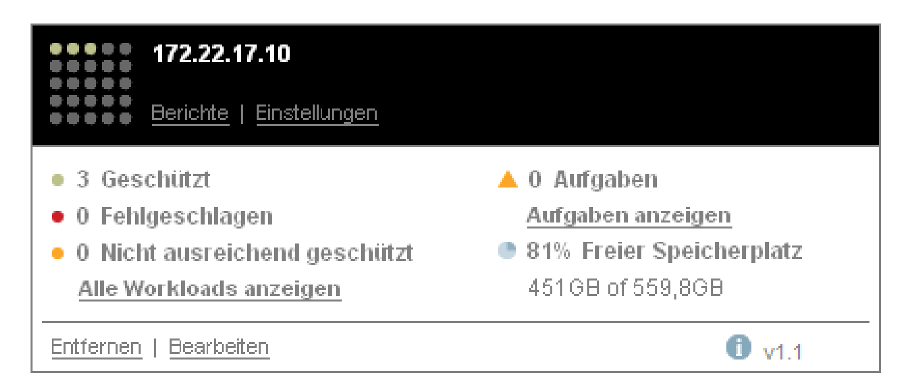
Abbildung 4-4 *Die Standardseite „Dashboard“ der Verwaltungskonsole*



4.5.2 Informationen zu PlateSpin Forge-Verwaltungskonsolenkarten

Einzelne Instanzen von PlateSpin Forge werden nach dem Hinzufügen zur Verwaltungskonsole als Karten dargestellt.

Abbildung 4-5 *PlateSpin Forge-Instanzkarte*



Eine Karte zeigt grundlegende Informationen über die spezifische Instanz von PlateSpin Forge an, z. B.:

- IP-Adresse/Hostname
- Standort
- Versionsnummer
- Workload-Anzahl
- Workload-Status

- Speicherkapazität
- Verbleibender freier Speicherplatz

Hyperlinks auf jeder Karte ermöglichen Ihnen die Navigation zu den für diese Instanz spezifischen Seiten „Workloads“, „Berichte“, „Einstellungen“ und „Aufgaben“. Es gibt darüber hinaus Hyperlinks, über die Sie die Konfiguration einer Karte bearbeiten oder eine Karte aus der Anzeige entfernen können.

4.5.3 Hinzufügen von PlateSpin Forge-Instanzen zur Verwaltungskonsole

Beim Hinzufügen einer PlateSpin Forge-Instanz zur Verwaltungskonsole wird eine neue Karte zum Dashboard der Verwaltungskonsole hinzugefügt.

Hinweis: Wenn Sie sich auf einer PlateSpin Forge-Instanz bei der Verwaltungskonsole anmelden, wird diese Instanz nicht automatisch zur Konsole hinzugefügt. Sie muss manuell hinzugefügt werden.

So fügen Sie eine PlateSpin Forge-Instanz zur Konsole hinzu:

1. Klicken Sie im Hauptdashboard der Konsole auf *Hinzufügen*.

   Die Seite *Hinzufügen/Bearbeiten* wird angezeigt.
2. Geben Sie die URL der Forge-VM an. Es wird sowohl das HTTP- als auch das HTTPS-Protokoll unterstützt.
3. (Optional) Aktivieren Sie das Kontrollkästchen *Berechtigungsnachweis der Verwaltungskonsole verwenden*, um denselben Berechtigungsnachweis zu verwenden, der von der Konsole verwendet wird. Wenn diese Option ausgewählt ist, füllt die Konsole automatisch das Feld *Domäne\Benutzername* aus.
4. Geben Sie im Feld *Domäne\Benutzername* einen Domänennamen und einen Benutzernamen ein, die für die von Ihnen hinzugefügte PlateSpin Forge-Instanz gültig sind. Geben Sie im Feld *Passwort* das entsprechende Passwort ein.
5. (Optional) Geben Sie einen beschreibenden oder identifizierenden *Anzeigenamen* (max. 15 Zeichen), einen *Speicherort* (max. 20 Zeichen) und ggf. erforderliche *Hinweise* ein (max. 400 Zeichen).
6. Klicken Sie auf *Hinzufügen/Speichern*.

   Es wird eine neue Karte zum Dashboard hinzugefügt.

4.5.4 Verwalten von Karten auf der Verwaltungskonsole

Sie können die Details einer PlateSpin Forge-Karte auf der Verwaltungskonsole ändern.

1. Klicken Sie auf den Hyperlink *Bearbeiten* auf der Karte, die Sie bearbeiten möchten.

   Die Seite *Hinzufügen/Bearbeiten* der Konsole wird angezeigt.
2. Nehmen Sie alle gewünschten Änderungen vor und klicken Sie anschließend auf *Hinzufügen/Speichern*.

   Das aktualisierte Konsolen-Dashboard wird angezeigt.

So entfernen Sie eine PlateSpin Forge-Karte von der Verwaltungskonsole:

1 Klicken Sie auf den Hyperlink *Entfernen* auf der Karte, die Sie entfernen möchten.

   Es wird eine Bestätigungsaufforderung angezeigt.

2 Klicken Sie auf *OK*.

   Die individuelle Appliance-Karte wird vom Dashboard entfernt.

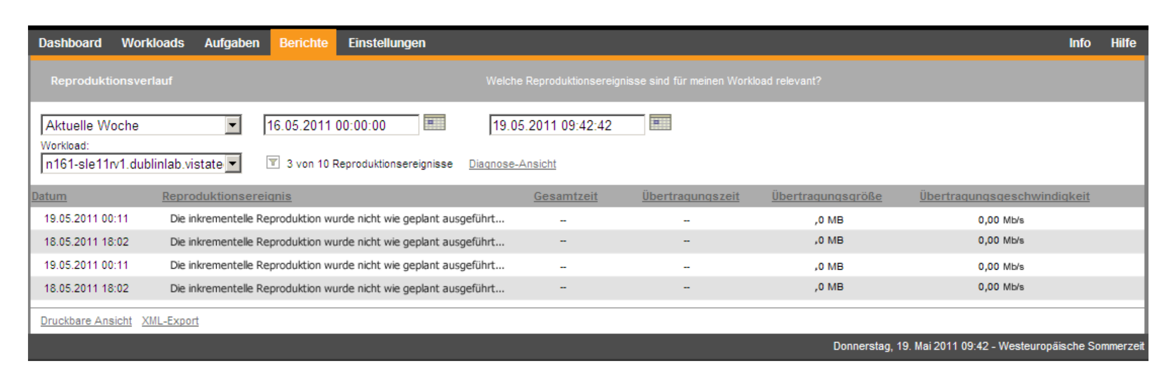
4.6 Generieren von Workload- und Workload-Schutz-Berichten

PlateSpin Forge ermöglicht Ihnen das Generieren von Berichten, die einen analytischen Einblick in Ihre Workload-Schutz-Zeitpläne über einen bestimmten Zeitraum hinweg gewähren.

Die folgenden Berichtstypen werden unterstützt:

- **Workload-Schutz:** Bericht über Reproduktionsereignisse für alle Workloads in einem auswählbaren Zeitraum.
- **Reproduktionsverlauf:** Bericht über Reproduktionstyp, Größe, Zeit und Übertragungsgeschwindigkeit pro auswählbarem Workload in einem auswählbaren Zeitraum.
- **Reproduktionsfenster:** Bericht über die Dynamik vollständiger und inkrementeller Reproduktionen, die nach *Durchschnitt*, *Zuletzt*, *Summe* und *Spitze* zusammengefasst werden können.
- **Aktueller Schutzstatus:** Statistikbericht über die Parameter *Ziel-RPO*, *RPO (tatsächlich)*, *TTO (tatsächlich)*, *RTO (tatsächlich)*, *Letzter Failover-Test*, *Letzte Reproduktion* und *Testalter*.
- **Ereignisse:** Bericht über Systemereignisse für alle Workloads in einem auswählbaren Zeitraum.
- **Routineereignisse:** Bericht über anstehende Workload-Schutz-Ereignisse.

***Abbildung 4-6** Optionen für einen Reproduktionsverlaufsbericht*



So erzeugen Sie einen Bericht:

1 Klicken Sie im PlateSpin Forge-Web-Client auf *Berichte*.

   Es wird eine Liste mit Berichtstypen angezeigt.

2 Klicken Sie auf den Namen des erforderlichen Berichtstyps.

Workload-Schutz

5

PlateSpin Forge erstellt eine Reproduktion Ihres Produktions-Workloads und aktualisiert diese Reproduktion regelmäßig auf Basis eines von Ihnen festgelegten Zeitplans.

Die Reproduktion bzw. der *Failover-Workload* ist eine virtuelle Maschine im VM-Container von PlateSpin Forge und übernimmt die Geschäftsfunktion des Produktions-Workloads, falls es zu einer Störung am Produktionsstandort kommt.

5.1 Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung

PlateSpin Forge definiert folgenden Workflow für den Workload-Schutz und die Wiederherstellung:

1 Vorbereitungsschritt:

1a Stellen Sie sicher, dass PlateSpin Forge Ihren Workload unterstützt.

Weitere Informationen hierzu finden Sie in „Unterstützte Konfigurationen“ auf Seite 11.

1b Stellen Sie sicher, dass Ihre Workloads die Zugriffs- und Netzwerkvoraussetzungen erfüllen.

Weitere Informationen hierzu finden Sie in „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“ auf Seite 23.

1c (nur Linux)

- (Bedingt) Wenn Sie planen, einen unterstützten Linux-Workload zu schützen, der einen nicht-standardmäßigen, benutzerdefinierten oder neueren Kernel hat, bauen Sie das PlateSpin `blkwatch`-Modul neu auf, das für eine Datenreproduktion auf Blockebene erforderlich ist.

  Weitere Informationen hierzu finden Sie im KB-Artikel 7005873 (http://www.novell.com/support/viewContent.do?externalId=7005873).

- (Empfohlen) Bereiten Sie LVM-Snapshots für den Datentransfer auf Blockebene vor. Stellen Sie sicher, dass jede Volume-Gruppe über genügend freien Speicherplatz für LVM-Snapshots verfügt (mindestens 10 % der Summe aller Partitionen).

  Weitere Informationen hierzu finden Sie im KB-Artikel 7005872 (http://www.novell.com/support/viewContent.do?externalId=7005872).

* (Optional) Legen Sie die benutzerdefinierten Skripts fest, die auf Ihrem Ursprungs-Workload bei jeder Reproduktion ausgeführt werden sollen, und bereiten Sie sie vor.

  Weitere Informationen hierzu finden Sie in „Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)“ auf Seite 88.

2 Fügen Sie einen Workload hinzu.

  Weitere Informationen hierzu finden Sie in „Hinzufügen eines Workloads für den Schutz“ auf Seite 60.

3 Konfigurieren Sie Schutzdetails und bereiten Sie die Reproduktion vor.

  Weitere Informationen hierzu finden Sie in „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“ auf Seite 61.

4 Starten Sie den Zeitplan für den Workload-Schutz.

  Weitere Informationen hierzu finden Sie unter „Starten des Workload-Schutzes“ auf Seite 64.

5 (Optional) Führen Sie manuell eine inkrementelle Reproduktion aus.

6 (Optional) Testen Sie die Failover-Funktionalität.

  Weitere Informationen hierzu finden Sie in Testen des Wiederherstellungs-Workloads und der Failover-Funktionalität.

7 Führen Sie einen Failover durch.

  Weitere Informationen hierzu finden Sie in „Failover“ auf Seite 65.

8 Führen Sie ein Failback durch.

  Weitere Informationen hierzu finden Sie unter „Failback“ auf Seite 68.

9 (Optional) Schützen Sie einen Workload nach einem Failback erneut.

Außer den Schritten 1, 8 und 9 können alle Schritte über Workload-Befehle auf der Seite „Workloads“ durchgeführt werden. Weitere Informationen hierzu finden Sie unter „Workloads und Workload-Befehle“ auf Seite 52.

Der Befehl *Erneut schützen* steht nach einem erfolgreichen Failback-Vorgang zur Verfügung.

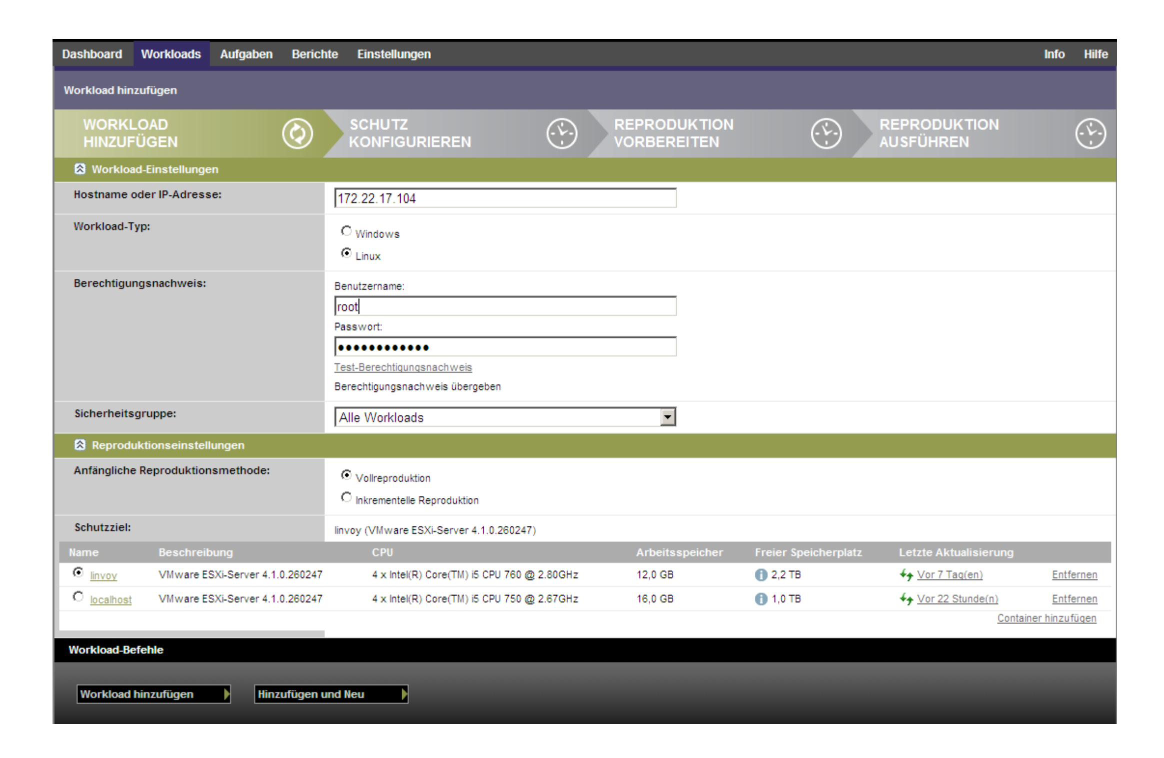
5.2 Hinzufügen eines Workloads für den Schutz

1 Führen Sie die erforderlichen Vorbereitungsschritte durch.

  Siehe Schritt 1 unter „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“ auf Seite 59.

2 Klicken Sie auf der Seite „Dashboard“ oder „Workloads“ auf *Workload hinzufügen*.

  Im PlateSpin Forge-Web-Client wird die Seite „Workload hinzufügen“ angezeigt.



3 Geben Sie die erforderlichen Workload-Details an:

- **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Workloads, das Betriebssystem, den Admin-Berechtigungsnachweis und eine Sicherheitsgruppe an, der der Workload zugewiesen werden soll. Weitere Informationen hierzu finden Sie in „Verwalten von PlateSpin Forge-Sicherheitsgruppen und -Workload-Berechtigungen“ auf Seite 22.

  Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter „Richtlinien für Workload-Berechtigungsnachweise“ auf Seite 83).

  Klicken Sie auf *Test-Berechtigungsnachweis*, um sicherzustellen, dass PlateSpin Forge auf den Workload zugreifen kann.

- **Reproduktionseinstellungen:** Wählen Sie die erforderlichen Reproduktionseinstellungen aus. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (Vollständig und Inkrementell)“ auf Seite 86.

4 Klicken Sie auf *Workload hinzufügen*.

PlateSpin Forge lädt die Seite „Workloads“ neu und blendet eine Fortschrittsanzeige für den Workload ein, der hinzugefügt wird . Warten Sie, bis der Vorgang abgeschlossen ist. Anschließend wird das Ereignis *Workload hinzugefügt* im Dashboard angezeigt.

5.3 Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion

Schutzdetails steuern die Workload-Schutz- und Wiederherstellungseinstellungen sowie das Verhalten im gesamten Lebenszyklus eines geschützten Workloads. In jeder Phase des Schutz- und Wiederherstellungs-Workflows (siehe „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“ auf Seite 59) werden relevante Einstellungen aus den Schutzdetails gelesen.

So konfigurieren Sie die Schutzdetails Ihres Workloads:

1. Fügen Sie einen Workload hinzu. Weitere Informationen hierzu finden Sie unter „Hinzufügen eines Workloads für den Schutz“ auf Seite 60.
2. Wählen Sie auf der Seite „Workloads“ den erforderlichen Workload aus und klicken Sie auf *Konfigurieren*.

   Im PlateSpin Forge-Web-Client wird die Seite „Schutzdetails“ des Workloads angezeigt.
3. Konfigurieren Sie die Schutzdetails in jeder Einstellungsgruppe so, wie sie für die Aufrechterhaltung Ihres ununterbrochenen Geschäftsbetriebs erforderlich sind. Weitere Informationen hierzu finden Sie unter „Workload-Schutz-Details“ auf Seite 62.
4. Beheben Sie alle Validierungsfehler.
5. Klicken Sie auf *Speichern*.

   Sie können alternativ auch auf *Speichern und vorbereiten* klicken. Dies speichert die Einstellungen und führt gleichzeitig den Befehl *Reproduktion vorbereiten* aus (bei Bedarf werden Datenübertragungstreiber auf dem Ursprungs-Workload installiert und die anfängliche VM-Reproduktion Ihres Workloads wird erstellt).

   Warten Sie, bis der Vorgang abgeschlossen ist. Anschließend wird das Ereignis *Workload-Konfiguration abgeschlossen* im Dashboard angezeigt.

5.3.1 Workload-Schutz-Details

Workload-Schutz-Details werden in fünf Parametergruppen angegeben:



Sie können jede Parametergruppe erweitern oder komprimieren, indem Sie auf das -Symbol auf der linken Seite klicken.

Im Folgenden sind die Details der fünf Parametergruppen aufgeführt:

Tabelle 5-1 *Workload-Schutz-Details*

Parametergruppe (Einstellungen)	Details
Ebene	Gibt die Schutzebene des aktuellen Schutzes an. Weitere Informationen hierzu finden Sie unter „Schutzebenen“ auf Seite 85.

<table>
<tr><th>Parametergruppe (Einstellungen)</th><th>Details</th></tr>
<tr><td>Reproduktion</td><td>Übertragungsverschlüsselung: Wählen Sie zum Aktivieren der Verschlüsselung die Option Datenübertragung verschlüsseln. Weitere Informationen hierzu finden Sie in „Sicherheit und Datenschutz“ auf Seite 12.

Übertragungsmethode: (Windows) Ermöglicht Ihnen, eine Datenübertragungsmethode und Sicherheit durch Verschlüsselung auszuwählen. Weitere Informationen hierzu finden Sie unter „Übertragungsmethoden“ auf Seite 84.

Ursprungsberechtigungsnachweis: Für den Zugriff auf den Workload erforderlich. Weitere Informationen hierzu finden Sie unter „Richtlinien für Workload-Berechtigungsnachweise“ auf Seite 83.

Anzahl der CPUs: Ermöglicht Ihnen die Angabe der erforderlichen Anzahl an dem Wiederherstellungs-Workload zugewiesenen vCPUs.

Reproduktionsnetzwerk: Ermöglicht Ihnen die Trennung des Reproduktionsdatenverkehrs auf der Basis virtueller Netzwerke, die auf Ihrem Appliance-Host definiert sind. Weitere Informationen hierzu finden Sie unter „Netzwerke“ auf Seite 90.

Datenablage für Wiederherstellungspunkte: Ermöglicht Ihnen die Auswahl einer mit Ihrem Appliance-Host verbundenen Datenablage zum Speichern von Wiederherstellungspunkten. Weitere Informationen hierzu finden Sie unter „Wiederherstellungspunkte“ auf Seite 86.

Geschützte Volumes: Verwenden Sie diese Optionen, um Volumes für den Schutz auszuwählen und deren Reproduktionen spezifischen Datenablagen auf Ihrem Appliance-Host zuzuweisen. Sie können für den Schutz auch folgende Elemente auswählen:

◆ Linux-Workloads: logische Volumes und Volume-Gruppen
◆ OES 2-Workloads: EVMS-Volumes

Weitere Informationen hierzu finden Sie in „Volumes“ auf Seite 89.

Thin-Festplatten-Option: Aktiviert die Funktion für virtuelle Thin-Provisioned-Datenträger, bei der ein virtueller Datenträger für die VM eine feste Größe zu haben scheint, jedoch nur die Menge an Festplattenspeicher verbraucht, die von diesem Datenträger benötigt wird.

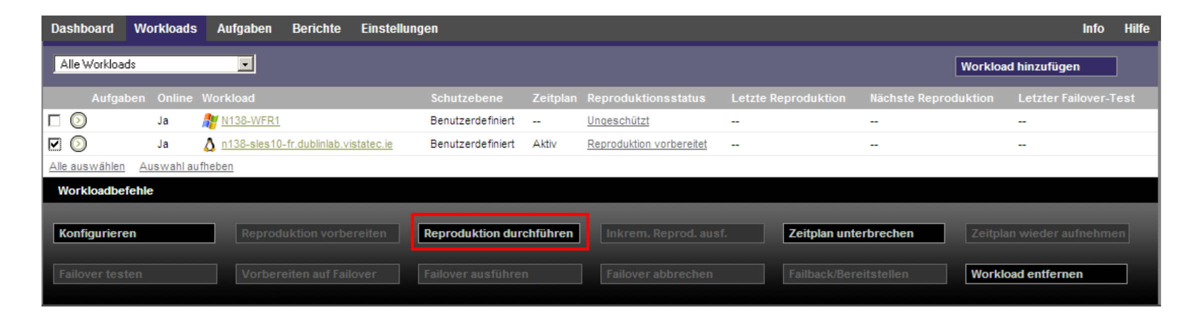
Dienste/Daemons, die während der Reproduktion angehalten werden sollen:

Ermöglicht Ihnen die Auswahl von Windows-Diensten oder Linux-Daemonen, die während der Reproduktion automatisch angehalten werden sollen. Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“ auf Seite 88.</td></tr>
</table>

Parametergruppe (Einstellungen)	Details
Failover	**VM-Arbeitsspeicher:** Ermöglicht Ihnen die Angabe der Menge an Arbeitsspeicher, der der Failover-VM zugeteilt werden soll. **Hostname und Domänen-/Arbeitsgruppenzugehörigkeit:** Verwenden Sie diese Optionen, um die Identität und Domänen-/Arbeitsgruppenzugehörigkeit des Failover-Workloads zu steuern, wenn dieser „live“ ist. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich. **Netzwerkverbindungen:** Verwenden Sie diese Optionen, um die LAN-Einstellungen des Failover-Workloads festzulegen. Weitere Informationen hierzu finden Sie unter „Netzwerke“ auf Seite 90. **Zu ändernde Dienst/Daemon-Status:** Ermöglicht Ihnen die Steuerung des Anfangsstatus spezifischer Anwendungsdienste (Windows) oder Daemons (Linux). Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“ auf Seite 88.
Vorbereiten auf Failover	Ermöglicht Ihnen die Steuerung der temporären Netzwerkeinstellungen des Failover-Workloads während des optionalen Vorgangs der Vorbereitung auf den Failover. Weitere Informationen hierzu finden Sie unter „Netzwerke“ auf Seite 90.
Failover testen	**VM-Arbeitsspeicher:** Ermöglicht Ihnen das Zuweisen des erforderlichen RAM zum temporären Workload. **Hostname:** Ermöglicht Ihnen das Zuweisen eines Hostnamens zum temporären Workload. **Domäne/Arbeitsgruppe:** Ermöglicht Ihnen die Zuordnung des temporären Workloads zu einer Domäne oder Arbeitsgruppe. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich. **Netzwerkverbindungen:** Steuert die LAN-Einstellungen des temporären Workloads. Weitere Informationen hierzu finden Sie unter „Netzwerke“ auf Seite 90. **Zu ändernde Dienst/Daemon-Status:** Ermöglicht Ihnen die Steuerung des Anfangsstatus spezifischer Anwendungsdienste (Windows) oder Daemons (Linux). Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“ auf Seite 88.

5.4 Starten des Workload-Schutzes

Der Workload-Schutz wird durch den Befehl *Reproduktion durchführen* gestartet:



Sie können den Befehl „Reproduktion durchführen“ nach folgenden Aktionen ausführen:

- Hinzufügen eines Workloads.
- Konfigurieren der Schutzdetails eines Workloads.
- Vorbereiten der anfänglichen Reproduktion.

Wenn Sie bereit sind, fortzufahren:

1. Wählen Sie auf der Seite „Workloads“ den erforderlichen Workload aus und klicken Sie auf *Reproduktion durchführen*.
2. Klicken Sie auf *Ausführen*.

   PlateSpin Forge startet die Ausführung und zeigt eine Fortschrittsanzeige für den Schritt *Daten kopieren* an.

Hinweis: Wenn ein Schutz-Vertrag erstellt wurde:

- Das Ändern der Größe eines Volumes, das auf Blockebene geschützt wird, macht den Schutz ungültig. Gehen Sie wie folgt vor: 1. Entfernen Sie den Vertrag. 2. Ändern Sie die Größe der Volumes, wie erforderlich. 3. Stellen Sie den Schutz wieder her.
- Nach jeder signifikanten Änderung des geschützten Workloads muss der Schutz neu hergestellt werden. Dies ist zum Beispiel erforderlich, wenn Volumes oder Netzwerkkarten zu einem geschützten Workload hinzugefügt wurden.

5.5 Failover

Failover ist der Vorgang, bei dem die Business-Funktion eines ausgefallenen Workloads von einem Wiederherstellungs-Workload innerhalb eines PlateSpin Forge-VM-Containers übernommen werden.

5.5.1 Fehlererkennung

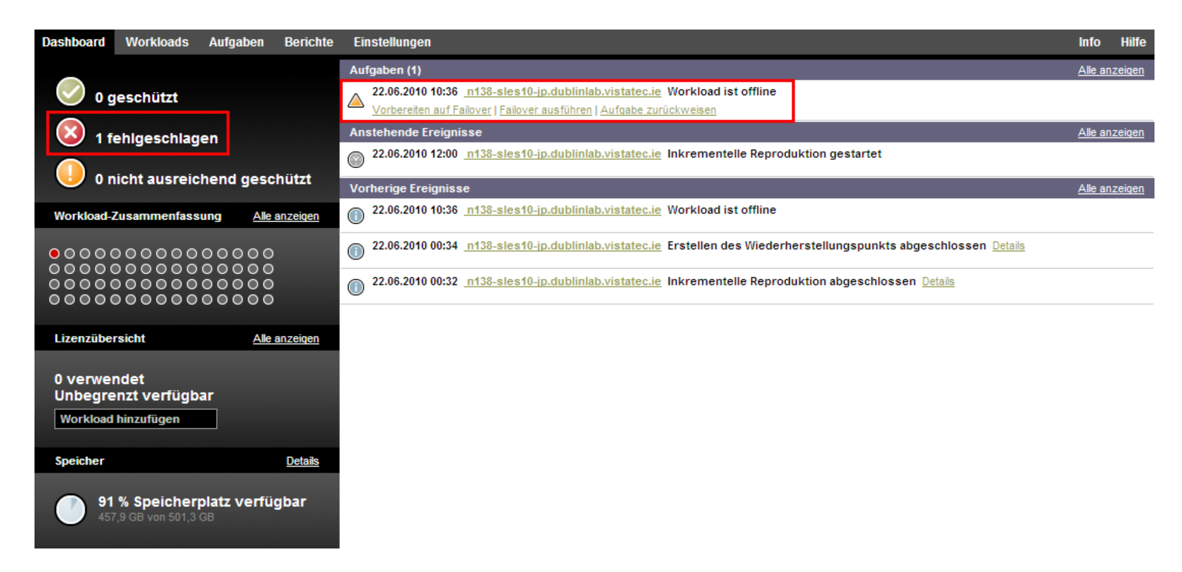
Wenn die festgelegte Anzahl an Versuchen, einen Workload zu erkennen, fehlschlägt, generiert PlateSpin Forge das Ereignis *Workload ist offline*. Kriterien, anhand derer ein Workload-Fehler definiert und protokolliert wird, sind Teil der Ebeneneinstellungen eines Workload-Schutzes (Informationen hierzu finden Sie in der Zeile Ebene unter „Workload-Schutz-Details“ auf Seite 62).

Wenn zusammen mit den SMTP-Einstellungen Benachrichtigungen konfiguriert wurden, sendet PlateSpin Forge gleichzeitig eine Benachrichtigungs-Email an die angegebenen Empfänger. Weitere Informationen hierzu finden Sie in „Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“ auf Seite 26.

Wenn ein Workload-Fehler erkannt wird, während der Status der Reproduktion *Im Leerlauf* lautet, können Sie mit dem Befehl *Failover ausführen* fortfahren. Wenn ein Workload-Fehler auftritt, während eine inkrementelle Reproduktion stattfindet, bleibt der Vorgang hängen. Brechen Sie in diesem Fall den Vorgang ab und fahren Sie dann mit dem Befehl *Failover ausführen* fort. Weitere Informationen hierzu finden Sie unter „Durchführen eines Failovers“ auf Seite 66.

Die folgende Abbildung zeigt die Dashboard-Seite des PlateSpin Forge-Web-Clients beim Erkennen eines Workload-Fehlers. Beachten Sie die anwendbaren Aufgaben im Teilfenster mit den Aufgaben und Ereignissen:

Abbildung 5-1 *Die Dashboard-Seite bei Erkennen eines Workload-Fehlers*



5.5.2 Durchführen eines Failovers

Failover-Einstellungen, einschließlich der Netzwerkidentitäts- und LAN-Einstellungen des Wiederherstellungs-Workloads, werden zum Zeitpunkt der Konfiguration zusammen mit den Schutzdetails gespeichert. Informationen hierzu finden Sie in der Zeile Failover unter „Workload-Schutz-Details“ auf Seite 62.

Sie können folgende Methoden zur Durchführung eines Failovers verwenden:

- Auswählen des erforderlichen Workloads auf der Seite „Workloads“ und Klicken auf *Failover ausführen*. Sie können den optionalen Befehl *Vorbereiten auf Failover* verwenden, um Ihre gespeicherten Failover-Einstellungen auf den Wiederherstellungs-Workload anzuwenden und diesen vor einem vollständigen Failover booten. Ziehen Sie einen getrennten *Vorbereiten auf Failover*-Vorgang in Erwägung, um sicherzustellen, dass Ihr Produktions-Workload wirklich ausgefallen ist. So sparen Sie Zeit, wenn Sie einen vollständigen *Failover*-Befehl ausführen.
- Klicken auf den entsprechenden Befehls-Hyperlink im Ereignis *Workload ist offline* im Teilfenster mit den Aufgaben und Ereignissen. Weitere Informationen hierzu finden Sie unter Abbildung 5-1.
- Manuelles Booten des Wiederherstellungs-Workloads mithilfe des VMware vSphere-Clients. Wählen Sie bei dieser Methode einen Snapshot (Wiederherstellungspunkt) mithilfe des Snapshot-Managers des vSphere-Clients aus.

  Weitere Informationen hierzu finden Sie in „Verwalten von Forge-Snapshots auf dem Appliance-Host“ auf Seite 44.

Hinweis: Wenn Sie einen Failover manuell durchführen, wendet das System die bei der Reproduktion des Workloads gespeicherten Failover-Einstellungen an.

Verwenden Sie eine dieser Methoden, um den Failover-Vorgang zu starten, und wählen Sie einen Wiederherstellungspunkt aus, der auf den Wiederherstellungs-Workload angewendet werden soll (siehe „Wiederherstellungspunkte“ auf Seite 86). Klicken Sie auf *Ausführen* und überwachen Sie den Vorgang. Wenn der Vorgang abgeschlossen ist, sollte der Reproduktionsstatus des Workloads *Live* lauten.

Informationen zum Testen des Wiederherstellungs-Workloads oder des Failover-Vorgangs im Rahmen einer geplanten Übung zur Wiederherstellung im Katastrophenfall finden Sie unter „Testen des Wiederherstellungs-Workloads und der Failover-Funktionalität“ auf Seite 67.

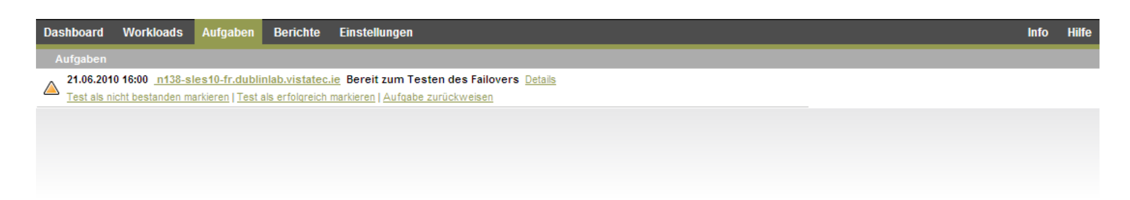
5.5.3 Testen des Wiederherstellungs-Workloads und der Failover-Funktionalität

PlateSpin Forge ermöglicht Ihnen, die Failover-Funktionalität und die Integrität des Wiederherstellungs-Workloads zu testen. Dies geschieht unter Verwendung des Befehls *Failover testen*, der den Wiederherstellungs-Workload zu Testzwecken in einer eingeschränkten Netzwerkumgebung bootet.

Wenn Sie diesen Befehl ausführen, wendet PlateSpin Forge die Failover-Test-Einstellungen, die in den Workload-Schutz-Details gespeichert sind, auf den Wiederherstellungs-Workload an (siehe Zeile Failover testen in „Workload-Schutz-Details“ auf Seite 62.

1. Definieren Sie ein angemessenes Zeitfenster für das Testen und stellen Sie sicher, dass keine Reproduktionen im Gange sind. Der Reproduktionsstatus des Workload muss *Im Leerlauf* sein.
2. Wählen Sie auf der Seite „Workloads“ den erforderlichen Workload aus, klicken Sie auf *Failover testen*, wählen Sie einen Wiederherstellungspunkt aus (siehe „Wiederherstellungspunkte“ auf Seite 86) und klicken Sie anschließend auf *Ausführen*.

   Anschließend generiert PlateSpin Forge ein entsprechendes Ereignis sowie eine Aufgabe mit einem Satz von anwendbaren Befehlen:

3. Überprüfen Sie die Integrität und betrieblichen Funktionen des Wiederherstellungs-Workloads. Verwenden Sie den VMware vSphere-Client, um auf den Wiederherstellungs-Workload im Appliance-Host zuzugreifen.

   Weitere Informationen hierzu finden Sie in „Herunterladen des VMware-Clientprogramms“ auf Seite 42.

4 Kennzeichnen Sie den Test als nicht bzw. als erfolgreich bestanden. Verwenden Sie die entsprechenden Befehle in der Aufgabe (*Test als nicht bestanden markieren*, *Test als erfolgreich markieren*). Die ausgewählte Aktion wird in dem Ereignisverlauf gespeichert, der dem Workload zugeordnet ist. *Aufgabe zurückweisen* verwirft die Aufgabe und das Ereignis.

Nach Abschluss der Aufgaben *Test als nicht bestanden markieren* oder *Test als erfolgreich markieren* verwirft PlateSpin Forge die temporären Einstellungen, die auf den Wiederherstellungs-Workload angewendet wurden. Der Schutz wird in den Zustand versetzt, den er vor dem Test hatte.

5.6 Failback

Der nächste logische Schritt, der einem Failover folgt, ist ein Failback-Vorgang. Er überträgt den Failover-Workload an seine ursprüngliche oder, falls erforderlich, auf eine neue Infrastruktur.

Failback-Methoden unterscheiden sich je nach Ziel-Infrastrukturtyp und dem Grad der Automatisierung des Failback-Vorgangs:

- **Automatischer Failback auf eine virtuelle Maschine:** Wird für VMware ESX-Plattformen unterstützt.
- **Halbautomatischer Failback auf einen physischen Computer:** Wird für alle physischen Computer unterstützt.
- **Halbautomatischer Failback auf eine virtuelle Maschine:** Wird für Xen auf SLES- und Microsoft Hyper-V-Plattformen unterstützt.

Die folgenden Abschnitte enthalten weitere Informationen:

- Abschnitt 5.6.1, „Automatischer Failback auf eine virtuelle Maschine“, auf Seite 68
- Abschnitt 5.6.2, „Halbautomatischer Failback auf einen physischen Computer“, auf Seite 71
- Abschnitt 5.6.3, „Halbautomatischer Failback auf eine virtuelle Maschine“, auf Seite 72

5.6.1 Automatischer Failback auf eine virtuelle Maschine

Die folgenden Container werden als Ziele für automatische Failbacks unterstützt:

Plattform	Hinweise
VMware DRS-Cluster in vSphere 4.1	• Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) • Der Cluster kann ESX 4.1, ESX**i** 4.1 oder beides verwenden
VMware ESX 3.5, 4.0, 4.1, 4.1 Update 1	
VMware ESX**i** 3.5, 4.0, 4.1, 4.1 Update 1	Alle ESX**i**-Versionen erfordern eine erworbene Lizenz. Der Schutz wird bei diesen Systemen nicht unterstützt, wenn sie mit einer kostenlosen Lizenz ausgeführt werden.

Führen Sie folgende Schritte aus, um einen automatischen Failback eines Failover-Workloads auf einen Ziel-VMware-Container durchzuführen.

1 Wählen Sie im Anschluss an einen Failover den Workload in der Seite „Workloads“ aus und klicken Sie auf *Failback durchführen/Bereitstellen*.

2 Legen Sie die folgenden Parametergruppen fest:

- **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Wiederherstellungs-Workloads und den Berechtigungsnachweis eines Administrators an. Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter „Richtlinien für Workload-Berechtigungsnachweise“ auf Seite 83).
- **Failback-Zieleinstellungen:** Legen Sie die folgenden Parameter fest:
  - **Reproduktionsmethode:** Wählen Sie den Umfang der Datenreproduktion aus. Wenn Sie *Inkrementell* auswählen, müssen Sie ein Ziel vorbereiten. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (Vollständig und Inkrementell)“ auf Seite 86.
  - **Zieltyp:** Wählen Sie *Virtuelles Ziel* aus. Falls Sie nicht über einen Failback-Container verfügen, klicken Sie auf *Container hinzufügen* und inventarisieren Sie einen unterstützten VM-Host. Verwenden Sie dazu einen Root-Berechtigungsnachweis.

3 Klicken Sie auf *Speichern und vorbereiten* und überwachen Sie den Fortschritt auf dem Bildschirm „Befehlsdetails“.

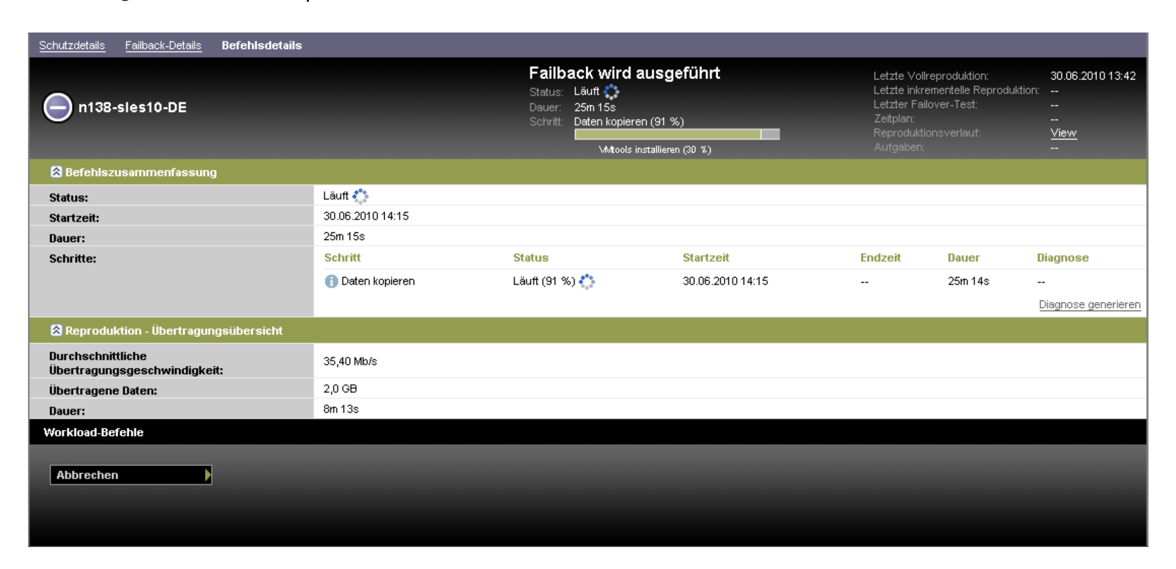
Nach erfolgreichem Abschluss lädt PlateSpin Forge den Bildschirm „Bereit für Failback“ und fordert Sie auf, die Details des Failback-Vorgangs anzugeben.

4 Konfigurieren Sie die Failback-Details. Weitere Informationen hierzu finden Sie unter „Failback-Details (Workload an VM)“ auf Seite 70.

5 Klicken Sie auf *Speichern und Failback durchführen* und überwachen Sie den Fortschritt auf der Seite „Befehlsdetails“. Weitere Informationen hierzu finden Sie unter Abbildung 5-2.

PlateSpin Forge führt den Befehl aus. Wenn Sie in der Parametergruppe "Post-Failback" den Parameter *Erneut schützen nach Failback* ausgewählt haben, wird der Befehl *Erneut schützen* im PlateSpin Forge-Web-Client angezeigt.

Abbildung 5-2 *Failback-Befehlsdetails*



Failback-Details (Workload an VM)

Failback-Details werden durch drei Parametergruppen dargestellt, die Sie konfigurieren, wenn Sie einen Workload-Failback an eine virtuelle Maschine durchführen.

Tabelle 5-2 *Failback-Details (VM)*

Parametergruppe (Einstellungen)	Details
Failback	**Übertragungsmethode:** (Windows) Ermöglicht Ihnen, eine Datenübertragungsmethode und Sicherheit durch Verschlüsselung auszuwählen. Weitere Informationen hierzu finden Sie unter „Übertragungsmethoden“ auf Seite 84.
	Failback-Netzwerk: Ermöglicht Ihnen, den Failback-Datenverkehr über ein dediziertes Netzwerk zu leiten, das zu den in IhremAppliance-Host definierten Netzwerken gehört. Weitere Informationen hierzu finden Sie unter „Netzwerke“ auf Seite 90.
	VM-Datenablage: Ermöglicht Ihnen die Auswahl einer Datenablage, die Ihrem Failback-Container für den Ziel-Workload zugeordnet ist.
	Zu kopierende Volumes: Ermöglicht Ihnen die Auswahl der Volumes für die Neuerstellung auf dem Ziel und die Zuweisung zu einer bestimmten Datenablage.
	Anzuhaltende Dienste/Daemonen: Ermöglicht Ihnen die Auswahl von Windows-Diensten oder Linux-Daemons, die während des Failbacks automatisch angehalten werden sollen. Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“ auf Seite 88.
	Alternative Adresse für Ursprung: Hier kann ggf. eine zusätzliche IP-Adresse für den Ursprungs-Workload eingegeben werden. Weitere Informationen hierzu finden Sie unter „Schutz über öffentliche und private Netzwerke durch NAT“ auf Seite 25.
Workload	***Anzahl der CPUs:*** Ermöglicht Ihnen die Angabe der erforderlichen Anzahl der dem Ziel-Workload zugewiesenen vCPUs.
	VM-Arbeitsspeicher: Ermöglicht Ihnen das Zuweisen des erforderlichen RAM zum Ziel-Workload.
	Hostname, Domäne/Arbeitsgruppe: Verwenden Sie diese Optionen, um die Identität und die Domänen-/Arbeitsgruppenzugehörigkeit des Ziel-Workloads zu steuern. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich.
	Netzwerkverbindungen: Verwenden Sie diese Optionen, um die Netzwerkzuordnung des Ziel-Workloads basierend auf den virtuellen Netzwerken des zugrunde liegenden VM-Containers anzugeben.
	Zu ändernde Dienststatus: Ermöglicht Ihnen die Steuerung des Anfangsstatus spezifischer Anwendungsdienste (Windows) oder Daemons (Linux). Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“ auf Seite 88.

Parametergruppe (Einstellungen)	Details
Post-Failback	**Workload erneut schützen:** Verwenden Sie diese Option, wenn Sie planen, den Schutzvertrag für den Ziel-Workload nach der Bereitstellung neu zu erstellen. Dadurch kann der Ereignisverlauf für den Workload kontinuierlich geführt und eine Workload-Lizenz automatisch zugewiesen/festgelegt werden. ◆ ***Erneut schützen nach Failback:*** Wählen Sie diese Option, wenn Sie planen, den Schutzvertrag für den Ziel-Workload neu zu erstellen. ◆ ***Kein erneutes Schützen:*** Wählen Sie diese Option, wenn Sie den Schutzvertrag für den Ziel-Workload nicht neu erstellen möchten.

5.6.2 Halbautomatischer Failback auf einen physischen Computer

Gehen Sie folgendermaßen vor, um nach einem Failover den Failback eines Workloads an einen physischen Computer durchzuführen. Bei dem physischen Computer kann es sich um die ursprüngliche oder eine neue Infrastruktur handeln.

1. Registrieren Sie den erforderlichen physischen Computer bei Ihrem PlateSpin Forge-Server. Weitere Informationen hierzu finden Sie in „Registrieren von physischen Computern mit PlateSpin Forge für Failback“ auf Seite 91.
2. (Optional: Windows-Plattformen) Führen Sie das PS-Analyseprogramm aus, um festzustellen, ob Treiber fehlen. Weitere Informationen hierzu finden Sie in „Analysieren von Workloads mit PlateSpin Analyzer (Windows)“ auf Seite 77.
3. Falls das PS-Analyseprogramm fehlende oder nicht kompatible Treiber meldet, laden Sie die erforderlichen Treiber in die Gerätetreiberdatenbank von PlateSpin Forge hoch. Weitere Informationen hierzu finden Sie unter „Verwalten der Gerätetreiber“ auf Seite 78.
4. Wählen Sie im Anschluss an einen Failover den Workload in der Seite „Workloads“ aus und klicken Sie auf *Failback durchführen/Bereitstellen*.
5. Legen Sie die folgenden Parametergruppen fest:
   - **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Wiederherstellungs-Workloads und den Berechtigungsnachweis eines Administrators an. Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter „Richtlinien für Workload-Berechtigungsnachweise“ auf Seite 83).
   - **Failback-Zieleinstellungen:** Geben Sie die folgenden Parameter an:
     - ***Reproduktionsmethode:*** Wählen Sie den Umfang der Datenreproduktion aus.

       Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (Vollständig und Inkrementell)“ auf Seite 86.
     - ***Zieltyp:*** Wählen Sie die Option *Physische Ziele* und wählen Sie anschließend den physischen Computer aus, den Sie in Schritt 1 registriert haben.
6. Klicken Sie auf *Speichern und vorbereiten* und überwachen Sie den Fortschritt auf dem Bildschirm „Befehlsdetails“.

   Nach erfolgreichem Abschluss lädt PlateSpin Forge den Bildschirm „Bereit für Failback“ und fordert Sie auf, die Details des Failback-Vorgangs anzugeben.

7 Konfigurieren Sie die Failback-Details und klicken Sie anschließend auf *Speichern und Failback durchführen*.

Überwachen Sie den Fortschritt auf dem Bildschirm „Befehlsdetails“.

5.6.3 Halbautomatischer Failback auf eine virtuelle Maschine

Bei diesem Failback-Typ wird ein Prozess ähnlich dem Halbautomatischer Failback auf einen physischen Computer für ein VM-Ziel durchgeführt, das kein nativ unterstützter VMware-Container ist. Während dieses Prozesses weisen Sie das System an, ein VM-Ziel als physischen Computer zu betrachten.

Ein halbautomatischer Failback auf eine VM wird für folgende Ziel-VM-Plattformen unterstützt:

- Xen unter SLES 10, 11
- Microsoft Hyper-V

5.7 Themen zu erweitertem Workload-Schutz

- Abschnitt 5.7.1, „Schützen von Windows-Clustern“, auf Seite 72
- Abschnitt 5.7.2, „Linux-Failback auf eine paravirtualisierte VM auf Xen unter SLES“, auf Seite 73

5.7.1 Schützen von Windows-Clustern

PlateSpin Forge unterstützt den Schutz der Geschäftsdienste eines Microsoft Windows-Clusters. Folgende Cluster-Technologien werden unterstützt:

- Auf Windows 2003 Server basierender Windows-Cluster-Server (*Single-Quorum Device Cluster*-Modell)
- Auf Windows 2008 Server basierendes Microsoft-Failover-Cluster (Modelle *Knoten- und Datenträgermehrheit* und *Keine Mehrheit: Nur Datenträger*)

Der Schutz eines Clusters wird durch inkrementelle Reproduktionen der Änderungen auf dem aktiven Knoten erreicht, die an ein virtuelles Einzelknoten-Cluster übertragen werden, das Sie während der Fehlerbehebung an der Ursprungsinfrastruktur verwenden können.

Der Umfang der Unterstützung von Cluster-Migrationen in der aktuellen Version ist von folgenden Bedingungen abhängig:

- Wenn Sie einen Vorgang des Typs *Workload hinzufügen* durchführen, müssen Sie über die IP-Adresse des Clusters (*Virtuelle IP-Adresse*) den aktiven Knoten identifizieren, d. h. den Knoten, der zurzeit die Quorum-Ressource des Clusters besitzt. Wenn Sie die IP-Adresse eines einzelnen Knotens angeben, wird dieser Knoten als regulärer Windows-Workload inventarisiert (das Cluster bleibt unerkannt).
- Eine Quorum-Ressource eines Clusters muss zu der Ressourcengruppe (Dienst) des Clusters gehören, die geschützt wird.

Wenn ein Knoten-Failover zwischen zwei inkrementellen Reproduktionen eines geschützten Clusters auftritt, generiert PlateSpin Forge ein Schutzereignis. Falls das Profil des neuen aktiven Knotens dem des ausgefallenen aktiven Knotens entspricht, wird der Zeitplan für den Schutz fortgesetzt, anderenfalls schlägt der Befehl fehl. Die Profile der Clusterknoten werden als ähnlich erachtet, wenn:

- sie dieselbe Anzahl an Volumes haben
- alle Volumes auf allen Knoten exakt dieselbe Größe haben
- sie eine identische Anzahl an Netzwerkverbindungen haben

Um ein Windows-Cluster zu schützen, gehen Sie nach dem gleichen Ablaufplan wie für den normalen Workload-Schutz vor (siehe „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“ auf Seite 59).

Beim Failback bietet PlateSpin Forge eine Validierung, die Ihnen hilft, sicherzustellen, dass auf dem Ziel freigegebene Volume-Layouts beibehalten werden. Stellen Sie sicher, dass Sie die Volumes ordnungsgemäß zuordnen.

5.7.2 Linux-Failback auf eine paravirtualisierte VM auf Xen unter SLES

Sie können ein Failback auf eine paravirtualisierte VM auf Xen unter SLES (nur Version 10) durchführen. Diese Migration erfolgt indirekt in zwei Phasen. Die paravirtualisierte VM muss zuerst in eine vollständig virtualisierte VM umgewandelt und später wieder zurückverwandelt werden. Zur Umwandlung der VM wird ein im PlateSpin Boot-ISO-Image enthaltenes Dienstprogramm (`xmps`) verwendet.

Das Verfahren variiert leicht, je nachdem, ob das Ziel eine neue oder eine vorhandene paravirtualisierte VM ist.

- „Linux-Failback auf eine neue paravirtualisierte VM“ auf Seite 73
- „Linux-Failback auf eine vorhandene paravirtualisierte VM“ auf Seite 75

Linux-Failback auf eine neue paravirtualisierte VM

1. Kopieren Sie das PlateSpin Linux Boot-ISO-Image auf den Xen/SLES-Zielserver. Weitere Informationen hierzu finden Sie in Tabelle 7-2, „ISO-Boot-Images für physische Zielcomputer“, auf Seite 91.
2. Starten Sie den Virtual Machine Manager und erstellen Sie eine vollständig virtualisierte VM:
   - **2a** Wählen Sie die Option *I need to install an operating system* (Ich muss ein Betriebssystem installieren).
   - **2b** Wählen Sie eine geeignete Größe für das Datenträger-Image (die Datenträgergröße sollte größer oder gleich der Datenträgergröße des Ursprungscomputers sein).
   - **2c** Wählen Sie das Boot-ISO-Image als Installationsquelle.

     Die VM bootet in der PlateSpin-Betriebssystemumgebung, die in den Einstellungen für das *Failback auf den physischen Computer* angegeben ist.
3. Führen Sie die Failback-Prozedur durch. Weitere Informationen hierzu finden Sie in „Halbautomatischer Failback auf einen physischen Computer“ auf Seite 71.

Wenn der Vorgang abgeschlossen ist, sollte die VM als vollständig virtualisierter Computer voll funktionsfähig sein.

4 Starten Sie die VM neu und achten Sie darauf, dass sie immer noch in die PlateSpin-Betriebssystemumgebung startet.

```
Welcome to PlateSpin/OS version 9.9.9.9

Available boot options (type the name to boot into):

  ps        - PlateSpin Linux for Taking Control (press ENTER to boot into)
  ps64      - PlateSpin Linux(x86_64) for Taking Control
  ps64_512m - PlateSpin Linux(x86_64) for Taking Control a Virtual Machine
              which has more than 512M memory
  next      - Boot from Next Boot Device Set in BIOS (timeout)
  debug     - PlateSpin Linux for Trouble Shooting
  switch    - PlateSpin Linux for switching kernel to Xen PV

  When no key is pressed for 20 seconds, it will boot from the next boot device.


boot: switch_
```

5 Geben Sie an der `boot:`-Eingabeaufforderung `switch` ein und drücken Sie die Eingabetaste.

Dadurch wird das Betriebssystem wieder als bootfähige paravirtualisierte Maschine konfiguriert. Wenn der Vorgang abgeschlossen ist, sollte die Ausgabe ähnlich wie die folgende aussehen:

```
about to find other volumes in native off-line OS
kjournald starting.  Commit interval 5 seconds
EXT3-fs: mounted filesystem with ordered data mode.
found volume /boot in off-line OS
found other 1 volume(s)
mount all the system volumes
kjournald starting.  Commit interval 5 seconds
EXT3 FS on hda1, internal journal
EXT3-fs: mounted filesystem with ordered data mode.
volume /boot has been mounted.
all the system volumes are mounted
Switching to Xen kernel for Para-virt machine....
unmount all the system volumes for clean up.
volume /boot has been unmounted
volume / has been unmounted

######################################################################
Please apply the following data as bootloader_args for
switching Xen fully-virt machine to Para-virt machine:

'--entry=xvda1:/vmlinuz-2.6.16.60-0.54.5-xen,/initrd-2.6.16.60-0.54.5-xen'

######################################################################

[DB]$ _
```

Beachten Sie die Bootloader-Argumente im letzten Abschnitt der Ausgabe:

```
Please apply the following data as bootloader_args for
switching Xen fully-virt machine to Para-virt machine:

'-entry=xvda1:/vmlinuz-2.6.16.60-0.54.5-xen, /initrd-2.6.16.60-0.54.5-
xen'
```

Diese werden vom `xmps`-Dienstprogramm verwendet, um den Speicherort des Kernels und des `initrd`-Images einzurichten, von dem aus die paravirtualisierte Maschine startet.

6 Schalten Sie die virtuelle Maschine aus:

```
[DB]$ poweroff
```

7. Melden Sie sich beim XEN/SLES-Server als `root` an und mounten Sie das PlateSpin Linux Boot-ISO-Image (das Befehlsbeispiel geht davon aus, dass das ISO-Image in das Verzeichnis `/root` kopiert wurde):

   ```
   # mkdir /mnt/ps
   # mount -o loop /root/linuxfailback.iso /mnt/ps
   ```

8. Führen Sie das `xmps`-Dienstprogramm aus, um eine paravirtualisierte VM auf der Basis der Konfiguration der vollständig virtualisierten VM zu erstellen:

   ```
   # /mnt/ps/tools/xmps --pv --vm_name=SLES10-FV --new_vm_name=SLES10-PV --
   bootloader_args="--entry=xvda1:/vmlinuz-2.6.16.60-0.54.5-xen, /initrd-
   2.6.16.60-0.54.5-xen"
   ```

   Geben Sie folgendes im Dienstprogramm ein:

   - den Namen der vollständig virtualisierten VM, auf der die Konfiguration der paravirtualisierten Maschine basieren soll (`SLES10-FV`)
   - den Namen der zu erstellenden virtuellen Maschine (`SLES10-PV`)
   - die Bootloader-Argumente der paravirtualisierten Maschine `"--bootloader_args"` (dargestellt unter Schritt 5)

   Wenn bereits eine VM mit demselben Namen wie der unter `new_vm_name` angegebene vorhanden ist, schlägt das `xmps`-Dienstprogramm fehl.

   Die neu erstellte paravirtualisierte VM (`SLES10-PV`) sollte nun im Virtual Machine Manager verfügbar und bereit zum Einschalten sein. Die entsprechende vollständig virtualisierte Maschine ist deaktiviert und kann nicht gebootet werden. Diese VM kann sicher gelöscht werden (nur die VM-Konfiguration wird entfernt).

9. Entladen Sie das PlateSpin Linux Boot-ISO-Image:

   ```
   # umount /mnt/ps
   ```

Linux-Failback auf eine vorhandene paravirtualisierte VM

1. Kopieren Sie das PlateSpin Linux Boot-ISO-Image auf den Xen/SLES-Zielserver. Weitere Informationen hierzu finden Sie in Tabelle 7-2, „ISO-Boot-Images für physische Zielcomputer“, auf Seite 91.

2. Melden Sie sich beim XEN/SLES-Server als `root` an und mounten Sie das PlateSpin Linux Boot-ISO-Image:

   ```
   # mkdir /mnt/ps
   # mount -o loop /root/linuxfailback.iso /mnt/ps
   ```

3. Führen Sie das `xmps`-Dienstprogramm aus, um eine vollständig virtualisierte VM auf der Basis der Konfiguration der paravirtualisierten VM (dem beabsichtigten Failback-Ziel) zu erstellen:

   ```
   # /mnt/ps/tools/xmps --fv --vm_name=SLES10-PV  --new_vm_name=SLES10-FV --
   bootiso=/root/linuxfailback.iso
   ```

   Geben Sie folgendes im Dienstprogramm ein:

   - den Namen der vorhandenen paravirtualisierten Maschine (`SLES10-PV`), die das beabsichtigte Failback-Ziel ist
   - den Namen der vorübergehend vollständig virtualisierte Maschine (`SLES10-FV`), die für den zweistufigen Failback-Vorgang erstellt werden soll
   - den vollständigen Pfad des Boot-ISO-Images (unter der Annahme, dass sich die ISO-Datei unter `/root: /root/booxofxx2p.iso` befindet)

Wenn bereits eine VM mit demselben Namen wie der unter `new_vm_name` angegebene vorhanden ist, schlägt das `xmps`-Dienstprogramm fehl.

Die neu erstellte vollständig virtualisierte VM (`SLES10-FV`) sollte nun im Virtual Machine Manager verfügbar sein.

4 Schalten Sie die neu erstellte vollständig virtualisierte Maschine (`SLES10-FV`) ein.

Die VM bootet in der PlateSpin-Betriebssystemumgebung, die in den Einstellungen für das *Failback auf den physischen Computer* angegeben ist.

5 Führen Sie die Failback-Prozedur durch. Weitere Informationen hierzu finden Sie in „Halbautomatischer Failback auf einen physischen Computer“ auf Seite 71.

6 Starten Sie die VM neu, führen Sie `switch` aus und konfigurieren Sie den Workload erneut, wie unter „Linux-Failback auf eine neue paravirtualisierte VM“ auf Seite 73 beschrieben (nur von Schritt 4 bis Schritt 9).

Hilfswerkzeuge für die Arbeit mit physischen Computern

6

Im Lieferumfang von PlateSpin Forge sind Werkzeuge enthalten, die für die Verwendung bei der Arbeit mit physischen Computern als Failback-Ziele vorgesehen sind.

- Abschnitt 6.1, „Analysieren von Workloads mit PlateSpin Analyzer (Windows)“, auf Seite 77
- Abschnitt 6.2, „Verwalten der Gerätetreiber“, auf Seite 78

6.1 Analysieren von Workloads mit PlateSpin Analyzer (Windows)

Verwenden Sie PlateSpin Analyzer, um potenzielle Treiberprobleme zu ermitteln, und beheben Sie diese, bevor Sie auf einem physischen Computer ein Workload-Failback oder einen Workload-Vorgang durchführen.

Hinweis: PlateSpin Analyzer unterstützt zurzeit nur Windows-Workloads.

---

1 Starten Sie auf der Forge-VM das Programm `Analyzer.Client.exe`, das sich in folgendem Verzeichnis befindet:

   `Programme\PlateSpin Forge Server\PlateSpin Analyzer`

2 Stellen Sie sicher, dass als Netzwerk *Standard* ausgewählt ist, und wählen Sie den erforderlichen Computer in der Dropdown-Liste *Alle Computer* aus.

3 (Optional) Beschränken Sie den Umfang der Computer auf eine bestimmte Sprache, um die Analysedauer zu verkürzen.

4 Klicken Sie auf *Analysieren*.

   Je nach Anzahl der inventarisierten Workloads, die Sie ausgewählt haben, kann die Analyse zwischen wenigen Sekunden und mehreren Minuten dauern.

Analysierte Server werden im linken Teilfenster aufgeführt. Wählen Sie einen Server aus, um die Testergebnisse im rechten Teilfenster anzuzeigen. Die Testergebnisse können sich aus allen oder einigen der folgenden Elemente zusammensetzen:

Tabelle 6-1 *Statusmeldungen in PlateSpin Analyzer-Testergebnissen*

Ergebnis	Beschreibung
Bestanden	Der Computer hat die PlateSpin Analyzer-Tests bestanden.
Warnhinweis	Ein oder mehrere Tests haben Warnmeldungen für den Computer zurückgegeben, die auf potenzielle Migrationsprobleme hinweisen. Klicken Sie auf den Hostnamen, um die Details dazu anzuzeigen.
Fehlgeschlagen	Ein oder mehrere Tests für diesen Computer sind fehlgeschlagen. Klicken Sie auf den Hostnamen, um die Details anzuzeigen und weitere Informationen zu erhalten.

Die Registerkarte *Zusammenfassung* enthält eine Liste mit den analysierten und nicht analysierten Computern sowie den Computern, die den Test bestanden oder nicht bestanden haben bzw. bei denen eine Fehlermeldung ausgegeben wurde.

Die Registerkarte *Testergebnisse* bietet folgende Informationen:

Tabelle 6-2 *Registerkarte „Testergebnisse“ von PlateSpin Analyzer*

Abschnitt	Details
System Test	Bestätigt, dass der Computer die Mindestanforderungen an Hardware und Betriebssystem erfüllt.
Hardware-Unterstützung	Prüft die Hardware-Kompatibilität des Workloads.
Zielhardware-Unterstützung	Prüft die Hardware-Kompatibilität bezüglich der Verwendung als physischen Zielcomputer.
Softwaretest	Sucht nach Anwendungen und Datenbanken, die für den Live-Transfer geschlossen werden müssen, um die Transaktionsintegrität zu gewährleisten.
Test auf inkompatible Anwendungen	Stellt sicher, dass Anwendungen, die den Migrationsprozess bekanntermaßen stören, nicht auf dem System installiert sind. Diese Anwendungen werden in der Datenbank für inkompatible Anwendungen gespeichert. Wählen Sie zum Hinzufügen, Löschen oder Bearbeiten von Einträgen in dieser Datenbank *Inkompatible Anwendung* im Menü *Werkzeuge*.

Die Registerkarte *Eigenschaften* enthält detaillierte Informationen über einen ausgewählten Computer.

6.2 Verwalten der Gerätetreiber

PlateSpin Forge wird mit einer Bibliothek an Gerätetreibern ausgeliefert. Die passenden Treiber werden automatisch auf den Ziel-Workloads installiert. Verwenden Sie das Dienstprogramm PlateSpin Analyzer, um zu prüfen, ob die erforderlichen Treiber verfügbar sind. Weitere Informationen hierzu finden Sie unter „Analysieren von Workloads mit PlateSpin Analyzer (Windows)“ auf Seite 77.

Falls PlateSpin Analyzer feststellt, dass Treiber fehlen oder nicht kompatibel sind, oder falls Sie für Ihre Zielinfrastruktur bestimmte Treiber benötigen, müssen Sie möglicherweise Treiber zur PlateSpin Forge-Treiberdatenbank hinzufügen (heraufladen).

- Abschnitt 6.2.1, „Verpacken von Gerätetreibern für Windows-Systeme“, auf Seite 79
- Abschnitt 6.2.2, „Verpacken von Gerätetreibern für Linux-Systeme“, auf Seite 79
- Abschnitt 6.2.3, „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Forge“, auf Seite 80

6.2.1 Verpacken von Gerätetreibern für Windows-Systeme

So verpacken Sie Ihre Windows-Gerätetreiber zum Heraufladen in die PlateSpin Forge-Treiberdatenbank:

1. Bereiten Sie alle abhängigen Gerätetreiberdateien (`*.sys`, `*.inf`, `*.dll` usw.) für Ihre Zielinfrastruktur und Ihr Zielgerät vor. Wenn Sie herstellerspezifische Treiber als `.zip`-Archiv oder als Programmdatei erhalten haben, extrahieren Sie diese zuerst.
2. Speichern Sie die Treiberdateien in separaten Ordnern mit einem eigenen Ordner pro Gerät.

Die Treiber können nun hochgeladen werden. Weitere Informationen hierzu finden Sie in „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Forge“ auf Seite 80.

Hinweis: Damit eine problemlose Durchführung Ihres Schutzauftrags und des Ziel-Workloads gewährleistet ist, sollten Sie nur digital signierte Treiber für die folgenden Systeme hochladen:

- Alle 64-Bit-Windows-Systeme
- 32-Bit-Versionen von Windows Vista- und Windows Server 2008 und Windows 7-Systemen

---

6.2.2 Verpacken von Gerätetreibern für Linux-Systeme

Wenn Sie ein Paket Ihrer Linux-Gerätetreiber erstellen möchten, um sie in die PlateSpin Forge-Treiberdatenbank heraufzuladen, können Sie hierfür ein benutzerdefiniertes Dienstprogramm verwenden, das im Linux Take Control ISO-Boot-Image enthalten ist. Weitere Informationen hierzu finden Sie unter Tabelle 7-2, „ISO-Boot-Images für physische Zielcomputer“, auf Seite 91.

1. Erstellen Sie auf einer Linux-Workstation ein Verzeichnis für Ihre Gerätetreiberdateien. Alle Treiber in dem Verzeichnis müssen für denselben Kernel und dieselbe Architektur sein.
2. Laden Sie das Boot-Image herunter und mounten Sie es.

   Geben Sie beispielsweise in der Annahme, dass das ISO-Image in das Verzeichnis `/root` kopiert wurde, folgende Befehle ein:

   ```
   # mkdir /mnt/ps
   # mount -o loop /root/linuxfailback.iso /mnt/ps
   ```
3. Kopieren Sie vom Unterverzeichnis `/tools` des gemounteten ISO-Images das Archiv `packageModules.tar.gz` in ein anderes Arbeitsverzeichnis und extrahieren Sie es.

   Wenn sich beispielsweise die `.gz`-Datei in Ihrem aktuellen Arbeitsverzeichnis befindet, geben Sie folgenden Befehl ein:

   ```
   tar -xvzf packageModules.tar.gz
   ```
4. Wechseln Sie zum Arbeitsverzeichnis und führen Sie folgenden Befehl aus:

   ```
   ./PackageModules.sh –d <Pfad-zum-Treiberverzeichnis> -o <Paketname>
   ```

   Ersetzen Sie <*Pfad-zum-Treiberverzeichnis*> mit dem aktuellen Pfad zum Verzeichnis, in dem Sie Ihre Treiberdateien gespeichert haben, und <*Paketname*> mit dem aktuellen Paketnamen im folgenden Format:

   `Treibername-Treiberversion-Dist-Kernelversion-Arch``.pkg`

   Beispiel: `bnx2x-1.48.107-RHEL4-2.6.9-11.EL-i686.pkg`

Das Paket kann nun hochgeladen werden. Weitere Informationen hierzu finden Sie unter „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Forge“ auf Seite 80.

6.2.3 Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Forge

Verwenden Sie den PlateSpin Treibermanager zum Hochladen von Gerätetreibern in die Treiberdatenbank.

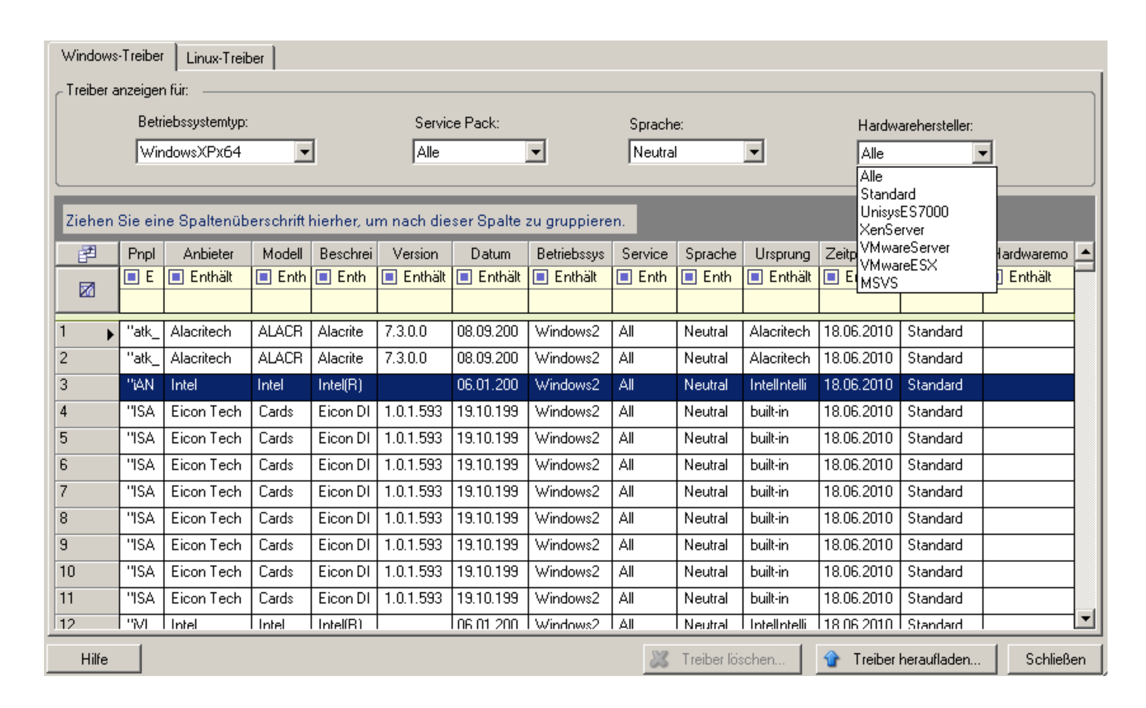
Hinweis: Beim Heraufladen von Treibern überprüft PlateSpin Forge nicht, ob der Treiber zum ausgewählten Betriebssystem bzw. den Bit-Spezifikationen passt. Laden Sie nur Treiber hoch, die für Ihre Zielinfrastruktur geeignet sind.

- „Upload-Prozedur für Gerätetreiber (Windows)“ auf Seite 80
- „Upload-Prozedur für Gerätetreiber (Linux)“ auf Seite 81

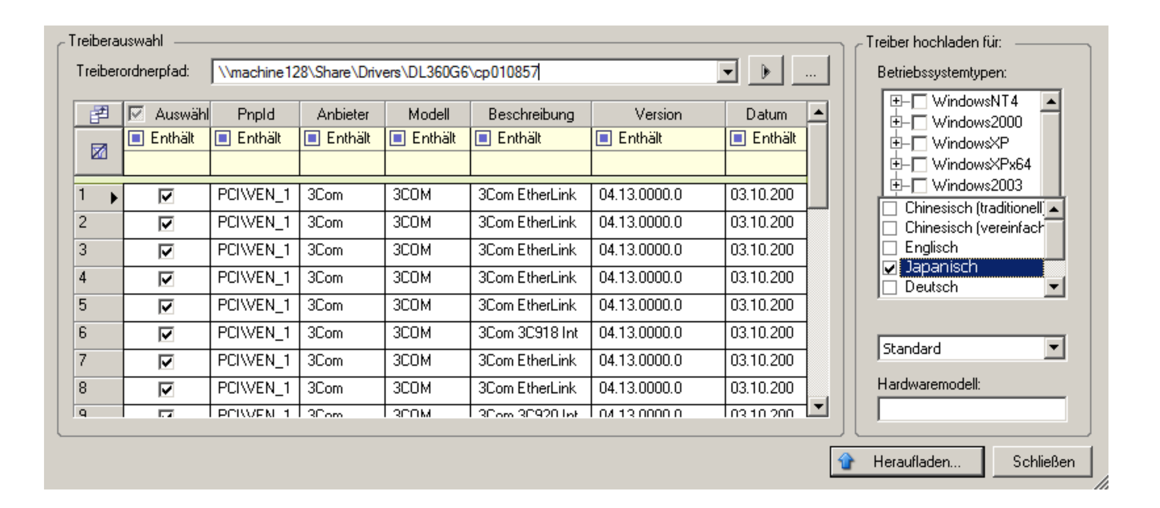
Upload-Prozedur für Gerätetreiber (Windows)

1 Beziehen Sie die erforderlichen Gerätetreiber und bereiten Sie diese vor. Weitere Informationen hierzu finden Sie in Verpacken von Gerätetreibern für Windows-Systeme.

2 Starten Sie auf Ihrer Forge-VM unter `Programme\PlateSpin Forge Server\DriverManager` das Programm `DriverManager.exe` und wählen Sie die Registerkarte *Windows-Treiber* aus.



3 Klicken Sie auf *Treiber hochladen*, navigieren Sie zu dem Ordner, der die erforderlichen Treiberdateien enthält, und wählen Sie den zutreffenden Betriebssystemtyp, die Sprache und die Hardwarehersteller-Optionen aus.



Wählen Sie *Standard* als Option für *Hardwarehersteller* aus, es sei denn, Ihre Treiber sind speziell für eine der aufgeführten Zielumgebungen vorgesehen.

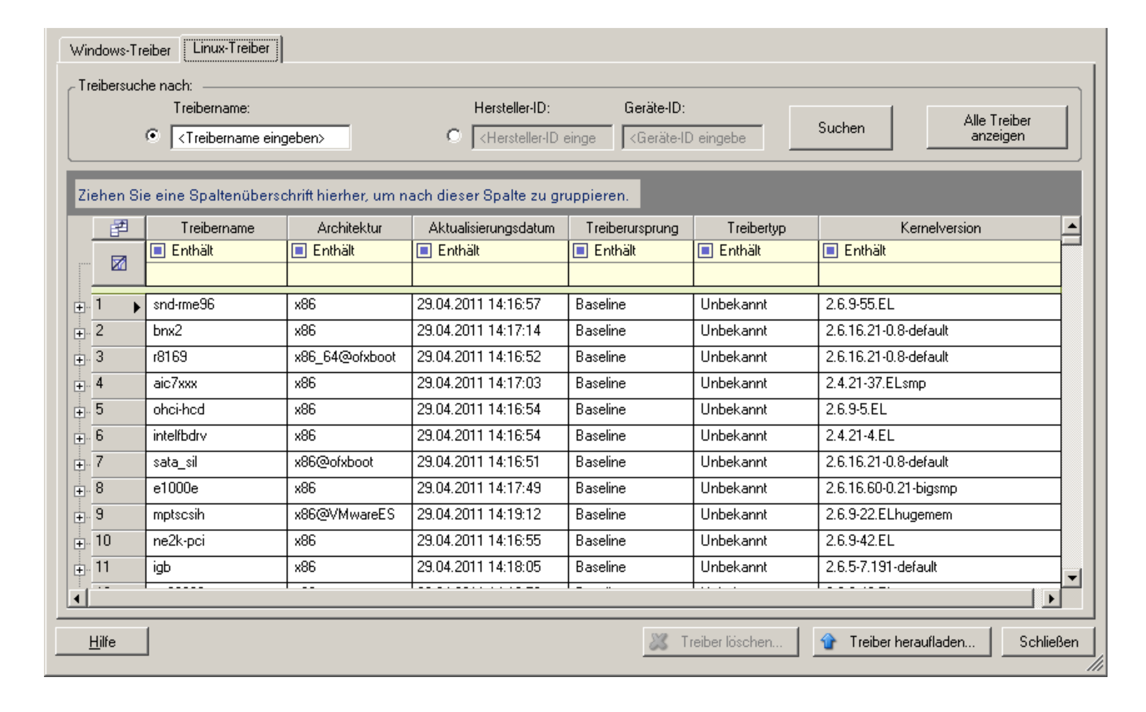
4 Klicken Sie auf *Heraufladen* und bestätigen Sie Ihre Auswahl.

Das System lädt die ausgewählten Treiber in die Treiberdatenbank.

Upload-Prozedur für Gerätetreiber (Linux)

1 Beziehen Sie die erforderlichen Gerätetreiber und bereiten Sie diese vor. Weitere Informationen hierzu finden Sie in Verpacken von Gerätetreibern für Linux-Systeme.

2 Klicken Sie auf *Werkzeuge* > *Gerätetreiber verwalten* und wählen Sie die Registerkarte *Linux-Treiber* aus:



3 Klicken Sie auf *Treiber hochladen*, navigieren Sie zu dem Ordner, der das erforderliche Treiberpaket (`*.pkg`) enthält, und klicken Sie auf *Alle Treiber hochladen*.

   Das System lädt die ausgewählten Treiber in die Treiberdatenbank.

Grundlagen des Workload-Schutzes

7

Dieser Abschnitt bietet Informationen zu den verschiedenen funktionalen Bereichen eines Workload-Schutzvertrags.

7.1 Richtlinien für Workload-Berechtigungsnachweise

PlateSpin Forge muss Administratorrechte für Workloads haben. Während des gesamten Workload-Schutz- und -Wiederherstellungs-Workflows werden Sie von PlateSpin Forge aufgefordert, Berechtigungsnachweise in einem bestimmten Format einzugeben.

Tabelle 7-1 *Workload-Berechtigungsnachweise*

Ermitteln von	Berechtigungsnachweis	Anmerkungen
Alle Windows-Workloads	Berechtigungsnachweis eines lokalen oder Domänen-Admins.	Verwenden Sie für den Benutzernamen das folgende Format: • Bei Domänenmitgliedscomputern: *Autorität\Prinzipal* • Bei Arbeitsgruppenmitgliedscomputern: *Hostname\Prinzipal*
Windows-Cluster	Domänen-Admin-Berechtigungsnachweis	Verwenden Sie die virtuelle IP-Adresse des Clusters. Wenn Sie die IP-Adresse eines einzelnen Knotens des Windows-Clusters verwenden, wird dieser Knoten als regulärer Windows-Workload ermittelt (das Cluster bleibt unerkannt).

Ermitteln von	Berechtigungsnachweis	Anmerkungen
Alle Linux-Workloads	Root-äquivalenter Benutzername und Passwort	Andere Konten als das Root-Konto müssen für die Verwendung von sudo konfiguriert werden. Weitere Informationen hierzu finden Sie im KB-Artikel 7920711 (http://www.novell.com/support/viewContent.do?externalId=7920711).
VMware ESX 4.1	ESX-Konto mit Admin-Rolle.	Wenn der ESX-Server 4.1 für die Windows-Domänenauthentifizierung konfiguriert ist, können Sie auch Ihren Berechtigungsnachweis für die Windows-Domäne verwenden.

7.2 Übertragungsmethoden

Eine Übertragungsmethode legt fest, wie Daten eines Ursprungs auf einem Ziel reproduziert werden. PlateSpin Forge bietet unterschiedliche Datenübertragungsmöglichkeiten, die vom Betriebssystem des geschützten Workloads abhängen:

- **Blockebene:** Daten werden auf dem Volume auf Blockebene reproduziert. Bei dieser Übertragungsmethode verwendet PlateSpin Forge einen Treiber zum Überwachen von Änderungen auf dem Ursprungs-Workload.
  - **Windows-Systeme:** Für Windows-Systeme verwendet PlateSpin Forge eine blockbasierte Komponente, die den Microsoft Volume Snapshot Service (VSS) mit Anwendungen und Diensten, die VSS unterstützen, nutzt. Bei der automatischen Installation der blockbasierten Komponente ist ein Neustart des Ursprungs-Workloads erforderlich (dies ist nicht der Fall, wenn Sie Windows-Cluster mit einem Datentransfer auf Blockebene schützen). Wenn Sie die Details zum Workload-Schutz konfigurieren, können Sie den Zeitpunkt der Komponenteninstallation auswählen. Wie beim Entfernen eines Workloads ist auch bei der Deinstallation der blockbasierten Komponente ein Neustart erforderlich.
  - **Linux-Systeme:** Transfers auf Blockebene auf Linux-Systemen werden von PlateSpin Forge mithilfe einer Datenübertragungskomponente auf Blockebene durchgeführt, die LVM-Snapshots nutzt, sofern vorhanden (die standardmäßige und empfohlene Option). Weitere Informationen hierzu finden Sie im KB-Artikel 7005872 (http://www.novell.com/support/viewContent.do?externalId=7005872).

    Die im Lieferumfang von PlateSpin Forge enthaltene blockbasierte Linux-Komponente ist für Standard- und Nicht-Debug-Kernels der unterstützen Linux-Distributionen vorkompiliert. Wenn Sie einen nicht-standardmäßigen, benutzerdefinierten oder neueren Kernel haben, können Sie die blockbasierte Komponente gemäß den Spezifikationen Ihres Kernels neu aufbauen. Weitere Informationen hierzu finden Sie im KB-Artikel 7005873 (http://www.novell.com/support/viewContent.do?externalId=7005873).

    Das Bereitstellen bzw. Entfernen der Komponente wird im Hintergrund ausgeführt, beeinträchtigt nicht die Kontinuität und erfordert keinen Benutzereingriff.
- **Dateiebene:** Die Daten werden dateiweise reproduziert (nur Windows). Dies wird mit und ohne VSS unterstützt.

PlateSpin Forge ermöglicht Ihnen, die Datenreproduktion zu verschlüsseln, um die Übertragung Ihrer Workload-Daten sicherer zu machen. Wenn die Verschlüsselung aktiviert ist, werden über das Netzwerk erfolgende Datentransfers vom Ursprung zum Ziel unter Verwendung von AES (Advanced Encryption Standard) oder 3DES, falls eine FIPS-konforme Verschlüsselung aktiviert ist.

Hinweis: Die Verschlüsselung wirkt sich auf die Leistung aus und kann die Datenübertragungsgeschwindigkeit erheblich beeinträchtigen.

7.3 Schutzebenen

Bei einer Schutzebene handelt es sich um eine benutzerdefinierbare Sammlung von Workload-Schutz-Parametern, die Folgendes definieren:

- Die Häufigkeit und das Wiederholungsmuster von Reproduktionen
- Ob und wie eine Datenkomprimierung durchgeführt werden soll
- Ob die verfügbare Bandbreite während des Datentransfers auf eine bestimmte Durchsatzrate gedrosselt werden soll
- Kriterien, anhand derer das System einen Workload als fehlgeschlagen erachtet

Eine Schutzebene ist ein wesentlicher Bestandteil jedes Workload-Schutzvertrages. In der Konfigurationsphase eines Workload-Schutzvertrages können Sie eine von mehreren integrierten Schutzebenen auswählen und ihre Attribute entsprechend den Anforderungen des spezifischen Schutzvertrages anpassen.

Sie können benutzerdefinierte Schutzebenen auch vorab erstellen:

1. Klicken Sie im PlateSpin Forge-Web-Client auf *Einstellungen* > *Schutzebenen* > *Schutzebene erstellen*.
2. Geben Sie die Parameter für die neue Schutzebene ein:

Name	Geben Sie einen Namen für die Ebene ein.
Inkrementelle Wiederholung	Geben Sie die Häufigkeit der inkrementellen Reproduktionen und das inkrementelle Wiederholungsmuster an. Sie können das Datum direkt in das Feld *Beginn der Wiederholung* eingeben oder auf das Kalendersymbol klicken, um ein Datum auszuwählen. Wählen Sie *Keine* als Wiederholungsmuster, wenn nie eine inkrementelle Reproduktion durchgeführt werden soll.
Vollständige Wiederholung	Geben Sie die Häufigkeit der Vollreproduktionen und das Muster der vollständigen Wiederholung an.
Sperrzeit:	Verwenden Sie diese Einstellungen zum Erzwingen einer Reproduktionssperrzeit. Ziehen Sie die Implementierung dieser Funktionalität zum Aussetzen von geplanten Reproduktionen während der Hauptauslastungszeiten oder zur Vermeidung von Konflikten zwischen VSS-fähigen Windows-Anwendungen und der VSS-Datenübertragungskomponente auf Blockebene in Erwägung. Klicken Sie zum Festlegen einer Sperrzeit auf *Bearbeiten* und wählen Sie ein Wiederholungsmuster (Täglich, Wöchentlich etc.) sowie die Anfangs- und Endzeit der Sperrzeit. **Hinweis:** Zu Beginn einer Sperrzeit bricht das System alle laufenden Reproduktionen ab.

Komprimierungsgrad	Diese Einstellungen legen fest, ob und wie Workload-Daten vor der Übertragung komprimiert werden. Weitere Informationen hierzu finden Sie in „Datenkomprimierung“ auf Seite 14. Wählen Sie eine der verfügbaren Optionen aus.*Schnell* verbraucht die wenigsten CPU-Ressourcen auf dem Ursprung, geht jedoch mit einer geringeren Komprimierung einher. *Maximal* verbraucht die meisten Ressourcen, erzielt aber auch eine höhere Komprimierung. *Optimal* liegt dazwischen und ist die empfohlene Option.
Bandbreitendrosselung	Diese Einstellungen steuern die Bandbreitendrosselung. Weitere Informationen hierzu finden Sie in „Bandbreitendrosselung“ auf Seite 14. Um die Bandbreite bei Reproduktionen auf eine bestimmte Rate zu drosseln, geben Sie den erforderlichen Durchsatzwert in Mb/s sowie das Zeitmuster ein.
Beizubehaltende Wiederherstellungspunkte	Geben Sie die Anzahl der beizubehaltenden Wiederherstellungspunkte für Workloads an, die diese Schutzebene verwenden. Weitere Informationen hierzu finden Sie unter „Wiederherstellungspunkte“ auf Seite 86. Bei einem Wert von `0` wird diese Funktion deaktiviert.
Workload-Fehler	Geben Sie an, wie viele Versuche zur Workload-Erkennung durchgeführt werden sollen, bis der Workload als fehlgeschlagen erachtet wird.
Workload-Erkennung	Geben Sie das Zeitintervall (in Sekunden) zwischen den Workload-Erkennungsversuchen an.

7.4 Wiederherstellungspunkte

Ein Wiederherstellungspunkt ist ein zu einem bestimmten Zeitpunkt erstellter Snapshot eines Workloads. Er ermöglicht es, einen reproduzierten Workload in einem bestimmten Zustand wiederherzustellen.

Sie können für jeden geschützten Workload bis zu 32 Wiederherstellungspunkte verwenden.

Wiederherstellungspunkte, die sich im Laufe der Zeit anhäufen, können dazu führen, dass der Speicherplatz von PlateSpin Forge nicht mehr ausreicht.

Informationen zum Entfernen von Wiederherstellungspunkten aus Ihrer Appliance finden Sie unter „Verwalten von Forge-Snapshots auf dem Appliance-Host“ auf Seite 44.

7.5 Anfängliche Reproduktionsmethode (Vollständig und Inkrementell)

Bei Workload-Schutz- und Failback-Vorgängen bestimmt der Parameter „Anfängliche Reproduktion“ den Umfang der Daten, die von einem Ursprung auf ein Ziel übertragen werden.

- **Vollständig:** Eine vollständige Volume-Übertragung erfolgt von einem Produktions-Workload auf dessen Reproduktion (der Wiederherstellungs-Workload) oder von einem Failover-Workload auf seine ursprüngliche virtuelle oder physische Infrastruktur.

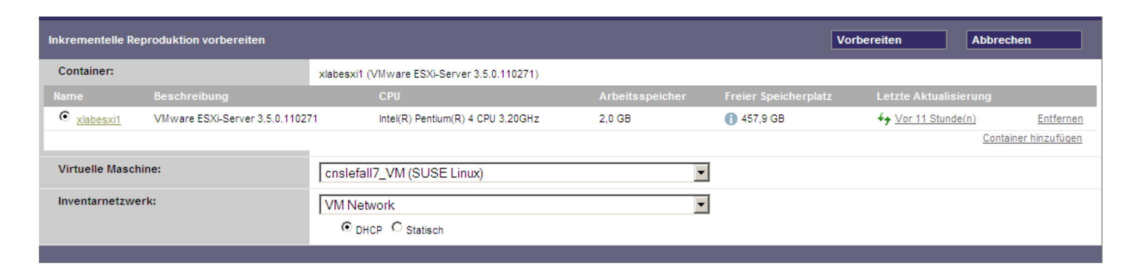
- **Inkrementell:** Es werden nur Unterschiede vom Ursprung eines ausgewählten Vorgangs auf dessen Ziel übertragen, vorausgesetzt, sie verfügen über ähnliche Betriebssysteme und Volume-Profile.
    - Beim Schutz: Der Produktions-Workload wird mit einer vorhandenen VM im Appliance-Host verglichen. Bei der vorhandenen VM kann es sich um eine der folgenden VMs handeln:
        - Die Wiederherstellungs-VM eines bereits geschützten Workloads (wenn die Option *VM löschen* des Befehls *Workload entfernen* deaktiviert wurde).
        - Eine VM, die manuell in den Appliance-Host importiert wurde, wie z. B. eine Workload-VM, die auf einem Wechseldatenträger physisch vom Produktionsstandort auf einen Remote-Wiederherstellungsstandort (nur für VMware ESX 3.5 und höher) verschoben wird.

          Weitere Informationen hierzu finden Sie in „Manuelles Importieren von VMs in die Datenablage des Appliance-Hosts“ auf Seite 45.
    - Während des Failbacks auf eine virtuelle Maschine wird der Failover-Workload mit einer vorhandenen VM in einem Failback-Container verglichen.
    - Während des Failbacks auf einen physischen Computer wird der Failover-Workload mit einem Workload auf einer physischen Zielmaschine verglichen, wenn der physische Computer in PlateSpin Forge registriert ist (siehe „Halbautomatischer Failback auf einen physischen Computer“ auf Seite 71).

Wenn Sie während des Workload-Schutzes und Failbacks auf einen VM-Host *Inkrementell* als anfängliche Reproduktionsmethode wählen, müssen Sie zur Ziel-VM navigieren und diese für eine Synchronisierung mit dem Ursprung des ausgewählten Vorgangs vorbereiten.

1. Fahren Sie mit dem erforderlichen Workload-Befehl fort, z. B. *Workload hinzufügen* oder *Failback*.
2. Wählen Sie für *Anfängliche Reproduktionsmethode* die Option *Inkrementelle Reproduktion*.
3. Klicken Sie auf *Workload vorbereiten*.

   Im PlateSpin Forge-Web-Client wird die Seite „Inkrementelle Reproduktion vorbereiten“ angezeigt.



4. Wählen Sie den erforderlichen Container, die virtuelle Maschine und das Inventarnetzwerk aus, das für die Kommunikation mit der VM verwendet werden soll.
5. Klicken Sie auf *Vorbereiten*.

   Warten Sie, bis der Prozess abgeschlossen wurde und darauf, dass die Benutzerschnittstelle zum ursprünglichen Befehl zurückkehrt, und wählen Sie den vorbereiteten Workload aus.

Hinweis: (Nur Datenreproduktionen auf Blockebene) Die erste inkrementelle Reproduktion dauert deutlich länger als nachfolgende Reproduktionen. Dies liegt daran, dass das System die Volumes auf dem Ursprung und dem Ziel Block für Block miteinander vergleichen muss. Nachfolgende Reproduktionen basieren auf Daten, die von der blockbasierten Komponente bereits abgefragt wurden, während sie einen Ursprung überwacht.

7.6 Steuerung von Diensten und Daemons

PlateSpin Forge ermöglicht Ihnen die Steuerung von Diensten und Daemons:

- **Steuerung des Diensts/Daemons:** Während des Datentransfers können Sie Windows-Dienste oder Linux-Daemons, die auf dem Ursprungs-Workload ausgeführt werden, automatisch anhalten. Dadurch wird sichergestellt, dass der Ursprungs-Workload in einem konsistenteren Zustand auf den Wiederherstellungs-Workload übertragen wird, als wenn die Dienste und Daemons weiterhin ausgeführt würden.

  Beispielsweise sollten Sie bei Windows-Workloads Dienste von Virenschutz-Software oder von VSS-Backup-Software anderer Hersteller anhalten.

  Um mehr Kontrolle über die Linux-Ursprünge während der Reproduktion zu haben, können Sie während jeder Reproduktion benutzerdefinierte Skripte über Ihre Linux-Workloads ausführen. Weitere Informationen hierzu finden Sie unter „Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)“ auf Seite 88.
- **Steuerung des Startstatus/der Ausführungsebene des Ziels:** Sie können den Startstatus (Windows) oder die Ausführungsebene (Linux) von Diensten/Daemons auf dem Ziel-Workload auswählen. Wenn Sie einen Failover-Vorgang oder einen Failover-Testvorgang ausführen, können Sie angeben, welche Dienste oder Daemons ausgeführt oder gestoppt werden sollen, wenn der Failover-Workload in den Live-Modus wechselt.

  Zu den allgemeinen Diensten, denen Sie den Startstatus () `Deaktiviert` zuweisen sollten, gehören herstellerspezifische Dienste, die an die ihnen zugrunde liegende physische Infrastruktur gebunden und in einer virtuellen Maschine nicht erforderlich sind.

7.7 Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)

Bei Linux-Systemen bietet PlateSpin Forge die Möglichkeit, die benutzerdefinierten Skripts `freeze` und `thaw` automatisch auszuführen. Diese Skripts ergänzen die automatische Daemon-Steuerungsfunktion. `freeze` wird zu Beginn einer Reproduktion ausgeführt, `thaw` am Ende.

Sie sollten diese Funktion in Ergänzung der automatisierten Daemon-Steuerungsfunktion verwenden, die über die Benutzeroberfläche zur Verfügung steht (siehe „Steuerung des Diensts/Daemons:“ auf Seite 88). Beispielsweise können Sie diese Funktion verwenden, um bestimmte Daemons während der Reproduktion temporär anzuhalten, statt sie herunterzufahren.

Führen Sie zur Implementierung der Funktion folgende Schritte aus, bevor Sie den Linux-Workload-Schutz einrichten:

1. Erstellen Sie die folgenden Dateien:
   - `platespin.freeze.sh`: Ein zu Beginn einer Reproduktion auszuführendes Shell-Skript

- `platespin.thaw.sh`: Ein zum Abschluss einer Reproduktion auszuführendes Shell-Skript
- `platespin.conf`: Eine Textdatei, die alle erforderlichen Argumente sowie einen Zeitüberschreitungswert definiert.

  Der Inhalt der Datei `platespin.conf` muss in folgender Syntax angegeben werden:

  ```
  [ServiceControl]
  FreezeArguments=<Argumente>
  ThawArguments=<Argumente>
  TimeOut=<Zeitüberschreitung>
  ```

  Ersetzen Sie <*Argumente*> durch die erforderlichen Befehlsargumente, getrennt durch ein Leerzeichen, und <*Zeitüberschreitung*> durch einen Zeitüberschreitungswert in Sekunden. Wenn kein Wert angegeben wurde, wird die Standard-Zeitüberschreitung (60 Sekunden) verwendet.

2 Speichern Sie die Skripte sowie die `.conf`-Datei auf dem Linux-Ursprungs-Workload in folgendem Verzeichnis:

```
/etc/platespin
```

7.8 Volumes

Beim Hinzufügen eines Workloads für den Schutz inventarisiert PlateSpin Forge die Speichermedien Ihres Ursprungs-Workloads und richtet automatisch Optionen im PlateSpin Forge-Web-Client ein, über die Sie die für den Schutz benötigten Volumes angeben können.

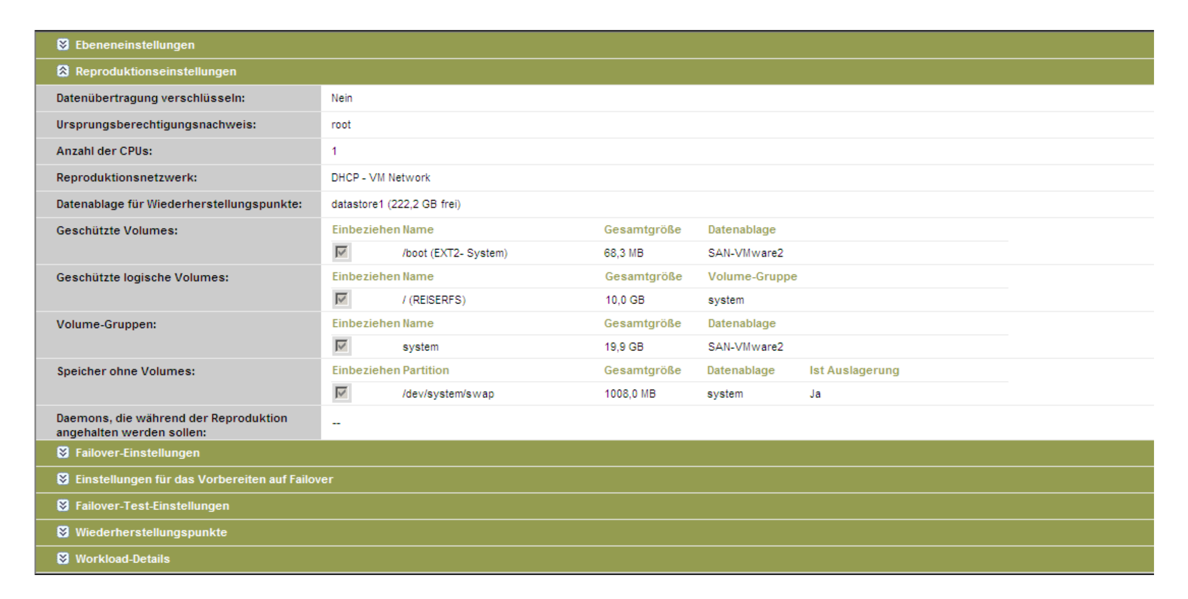
PlateSpin Forge unterstützt mehrere Speichertypen, darunter dynamische Windows-Datenträger, LVM, RAID und SAN.

Bei Linux-Workloads bietet PlateSpin Forge folgende zusätzlichen Funktionen:

- Nicht auf Volumes befindlicher Speicher, der dem Ursprungs-Workload zugeordnet ist, wird neu erstellt und dem Wiederherstellungs-Workload zugewiesen.
- Das Layout der Volume-Gruppen und logischen Volumes wird beibehalten, sodass Sie es während des Failbacks neu erstellen können.
- (OES 2-Workloads) EVMS-Layouts von Ursprungs-Workloads werden beibehalten und im Appliance-Host neu erstellt. NSS-Pools werden vom Ursprung in die Wiederherstellungs-VM kopiert.

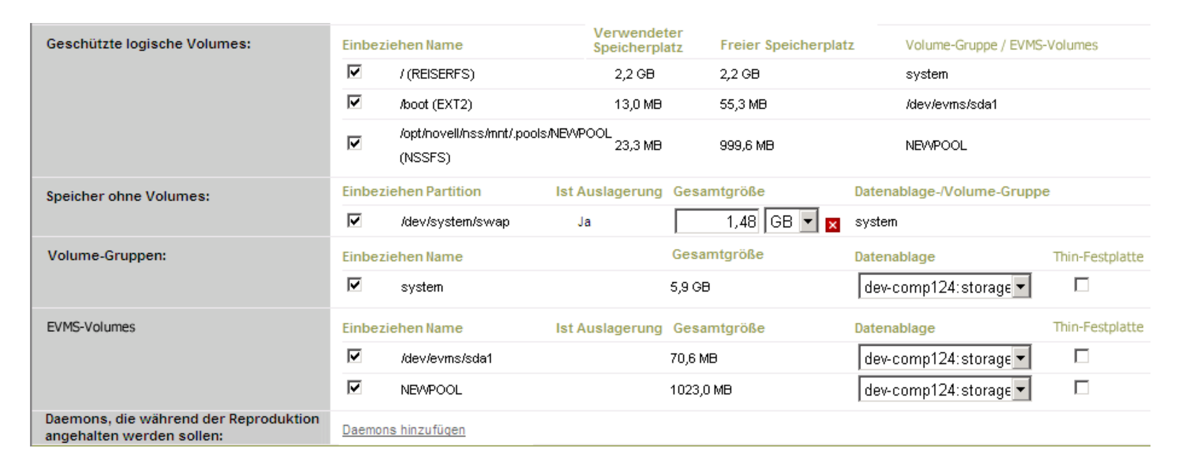
Die folgende Abbildung zeigt die unter „Reproduktionseinstellungen“ festgelegten Parameter für einen Linux-Workload mit mehreren Volumes und zwei logischen Volumes in einer Volume-Gruppe.

Abbildung 7-1 *Volumes, logische Volumes und Volume-Gruppen eines geschützten Linux-Workloads*



Die folgende Abbildung zeigt Volume-Schutz-Optionen eines OES 2-Workloads mit Optionen, die angeben, dass das EVMS-Layout beibehalten und für das Wiederherstellungs-Workload neu erstellt werden soll:

Abbildung 7-2 *Reproduktionseinstellungen, Volume-bezogene Optionen (OES 2-Workload)*



7.9 Netzwerke

PlateSpin Forge ermöglicht Ihnen die Steuerung der Netzwerkidentität Ihres Wiederherstellungs-Workloads und der LAN-Einstellungen, sodass Sie verhindern können, dass der Reproduktionsdatenverkehr den LAN- oder WAN-Datenverkehr beeinträchtigt.

Sie können spezifische Netzwerkeinstellungen in den Details für den Workload-Schutz festlegen, die in unterschiedlichen Phasen des Workload-Schutz- und -Wiederherstellungs-Workflows verwendet werden:

- **Reproduktion:** (Reproduktion-Parameter festgelegt) Zur Trennung des regulären Reproduktionsdatenverkehrs vom Produktionsdatenverkehr.
- **Failover:** (Failover-Parameter festgelegt) Definiert, dass der Wiederherstellungs-Workload beim Wechsel in den Live-Modus Teil des Produktionsnetzwerks wird.
- **Vorbereiten auf Failover:** (Vorbereiten auf Failover-Netzwerkparameter) Für Netzwerkeinstellungen während der optionalen Failover-Vorbereitungsphase.
- **Failover testen:** (Failover testen-Parameter festgelegt) Definiert, dass Netzwerkeinstellungen während einer Failover-Testphase für den Wiederherstellungs-Workload gelten.

7.10 Registrieren von physischen Computern mit PlateSpin Forge für Failback

Wenn die erforderliche Zielinfrastruktur für einen Failback-Vorgang ein physischer Computer ist, müssen Sie ihn in PlateSpin Forge registrieren.

Die Registrierung eines physischen Computers erfolgt durch das Booten des physischen Zielcomputers mit dem entsprechenden PlateSpin-Boot-Image (ISO-Image).

Wenn Sie ein Boot-ISO-Image verwenden möchten, laden Sie es vom PlateSpin Forge-Bereich der Novell-Downloadseite (http://download.novell.com/Download?buildid=C3BckY0Hp0s) herunter. Verwenden Sie das für Ihren Zielcomputer passende Image:

***Tabelle 7-2** ISO-Boot-Images für physische Zielcomputer*

Dateiname	Anmerkungen
`WindowsFailback.zip` (enthält `WindowsFailback.iso`)	Windows
`LinuxFailback.zip` (enthält `LinuxFailback.iso`)	Linux-Systeme
`WindowsFailback-Cisco.zip` (enthält `WindowsFailback-Cisco.iso`)	Windows-Systeme auf Cisco-Hardware
`WindowsFailback-Dell.zip` (enthält `WindowsFailback-Dell.iso`)	Windows-Systeme auf Dell-Hardware
`WindowsFailback-Fujitsu.zip` (enthält `WindowsFailback-Fujitsu.iso`)	Windows-Systeme auf Fujitsu-Hardware

Nachdem Sie die erforderliche Datei heruntergeladen haben, dekomprimieren Sie diese und speichern Sie die extrahierte ISO-Datei.

- Abschnitt 7.10.1, „Registrieren physischer Zielcomputer“, auf Seite 92

7.10.1 Registrieren physischer Zielcomputer

1. Brennen Sie das entsprechende Image auf eine CD oder speichern Sie es auf einem Medium, von dem Ihr Ziel booten kann.
2. Stellen Sie sicher, dass der Netzwerk-Switch-Anschluss, der mit dem Ziel verbunden ist, auf *Autom. Vollduplex* eingestellt ist.

   Da die Windows-Version des Boot-CD-Images nur die Funktion *Vollduplex automatisch aushandeln* unterstützt, wird hierdurch sichergestellt, dass keine Konflikte in den Duplexeinstellungen bestehen.
3. Verwenden Sie die Boot-CD zum Booten des physischen Zielcomputers und warten Sie, bis das Befehlszeilenfenster geöffnet wird.

   (Nur Windows) Warten Sie, bis die Befehlszeilenfenster *REGISTERMACHINE* und *Recovery Console* geöffnet sind. Verwenden Sie das Befehlszeilenfenster von REGISTERMACHINE. Weitere Informationen zum Befehlszeilenprogramm „Recovery Console“ finden Sie unter „Verwenden des Befehlszeilenprogramms „Recovery Console“ (Windows)“ auf Seite 93.
4. (Nur Linux) Geben Sie bei 64-Bit-Systemen im anfänglichen Bootprompt Folgendes ein:
   - `ps64` (für Systeme mit bis zu 512 MB RAM)
   - `ps64_512m` (für Systeme mit mehr als 512 MB RAM)
5. Drücken Sie die Eingabetaste.
6. Geben Sie bei der entsprechenden Aufforderung die folgende URL ein:

   `http://<Hostname | IP-Adresse>/platespinforge`

   Ersetzen Sie <*Hostname* | *IP-Adresse*> durch den Hostnamen bzw. die IP-Adresse Ihrer Forge-VM.
7. Geben Sie den Administrator-Berechtigungsnachweis für die Forge-VM einschließlich einer Zertifizierungsstelle an. Verwenden Sie für das Benutzerkonto das folgende Format:

   Domäne\Benutzername oder *Hostname\Benutzername*

   Verfügbare Netzwerkkarten werden anhand ihrer MAC-Adressen erkannt und angezeigt.
8. Wenn DHCP auf der zu verwendenden NIC verfügbar ist, drücken Sie die Eingabetaste, um fortzufahren. Wenn DHCP nicht verfügbar ist, geben Sie an, dass die erforderliche NIC mit einer statischen IP-Adresse konfiguriert werden soll.
9. Geben Sie einen Hostnamen für den physischen Computer ein oder drücken Sie die Eingabetaste, um die Standardwerte zu übernehmen.
10. Geben Sie *Ja* ein, wenn Sie SSL aktiviert haben. Andernfalls geben Sie *Nein* ein.

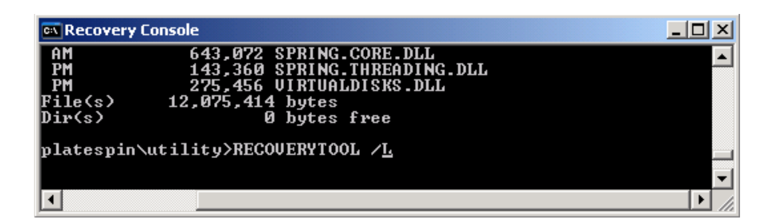
Nach kurzer Zeit sollte der physische Computer in den Failback-Einstellungen des PlateSpin Forge Web Clients verfügbar sein.

Verwenden des Befehlszeilenprogramms „Recovery Console“ (Windows)

Das Befehlszeilenprogramm „Recovery Console“ ermöglicht es Ihnen, Windows-Gerätetreiber dynamisch auf dem Zielcomputer einzubinden, ohne den gesamten Registrierungsprozess für das physische Ziel neu starten zu müssen.

Das Dienstprogramm wird beim ersten Versuch, vom Windows-Boot-Image zu starten, in einem zweiten Befehlszeilenfenster geladen (siehe Schritt 3 auf Seite 92).

Geben Sie zur Verwendung des Recovery-Tools den Befehlsnamen RECOVERYTOOL, gefolgt vom anwendbaren Parameter, im Recovery Console-Fenster ein.



Sie können folgende Parameter verwenden:

- /L - zum Auflisten aller auf dem Ziel-Betriebssystem installierten Treiberdienste
- /J - zum Einbinden von Treibern in das Ziel-Betriebssystem

Sie können angeben, ob die Treiber vom PlateSpin Forge-Server oder von einem lokalen Pfad heruntergeladen werden sollen. Wenn Sie einen lokalen Pfad verwenden möchten, sollten Sie mehrere Treiber für dasselbe Gerät gruppieren. Wenn Sie Treiber vom PlateSpin Forge-Server herunterladen möchten, fordert das Dienstprogramm Sie auf, anzugeben, welchen Treiber Sie verwenden möchten (falls es mehrere gibt).

Einfügen von Treibern in das PlateSpin-Boot-Image (Linux)

Sie können mithilfe eines benutzerdefinierten Dienstprogramms weitere Linux-Gerätetreiber zu einem Paket zusammenstellen und in das PlateSpin-Boot-Image einfügen, bevor Sie es auf eine CD brennen:

1. Besorgen Sie die erforderlichen *.ko-Treiberdateien oder kompilieren Sie sie.

   Wichtig: Stellen Sie sicher, dass die Treiber mit dem in der ISO-Datei (2.6.16.21-0.8-default) enthaltenen Kernel kompatibel sind und zur Architektur des Zielcomputers passen.

2. Mounten Sie das Image in einem Linux-Computer (root-Berechtigungsnachweis erforderlich). Verwenden Sie die folgende Befehlssyntax:

   ```
   mount –o loop <Pfad-zu-ISO> <Mount-Punkt>
   ```

3. Kopieren Sie das Skript rebuildiso.sh, das sich im Unterverzeichnis /tools der gemounteten ISO-Datei befindet, in ein temporäres Arbeitsverzeichnis. Wenn Sie fertig sind, entladen Sie die ISO-Datei. (Führen Sie dazu den Befehl unmount *<Mount-Punkt>* aus.)
4. Erstellen Sie ein weiteres Arbeitsverzeichnis für die erforderlichen Treiberdateien und speichern Sie diese in diesem Verzeichnis.
5. Führen Sie in dem Verzeichnis, in dem Sie das Skript rebuildiso.sh gespeichert haben, folgenden Befehl als Root-Benutzer aus:

```
./rebuildiso.sh –i <ISO-Datei> -d <Treiber-Verzeichnis> -m i586|x86_64
```

Wenn der Vorgang abgeschlossen ist, enthält die ISO-Datei die zusätzlichen Treiber.

Fehlersuche

8

8.1 Fehlerbehebung bei der Workload-Inventarisierung (Windows)

Möglicherweise müssen Sie die folgenden typischen Probleme während der Workload-Inventarisierung beheben.

Probleme oder Meldungen	Lösungen
`The domain in the credentials is invalid or blank`	Dieser Fehler tritt auf, wenn das Format des Berechtigungsnachweises falsch ist. Versuchen Sie, die Ermittlung unter Verwendung eines lokalen Administratorkontos mit dem Berechtigungsnachweisformat `Hostname\LocalAdmin` durchzuführen. Sie können auch versuchen, die Ermittlung unter Verwendung eines Domänen-Administratorkontos mit dem Berechtigungsnachweisformat `Domäne\DomainAdmin` durchzuführen.
`Unable to connect to Windows server...Access is denied`	Beim Versuch, einen Workload hinzuzufügen, wurde ein Nicht-Administratorkonto verwendet. Verwenden Sie ein Administratorkonto oder fügen Sie den Benutzer zur Administratorgruppe hinzu und versuchen Sie es erneut. Diese Meldung kann auch auf einen WMI-Verbindungsfehler hinweisen. Probieren Sie die nachfolgend aufgeführten Lösungsmöglichkeiten aus und führen Sie dann den „WMI-Verbindungstest“ auf Seite 97 erneut durch. Wenn der Test erfolgreich ist, versuchen Sie erneut, den Workload hinzuzufügen. ◆ „Fehlerbehebung bei DCOM-Verbindungen“ auf Seite 97 ◆ „Fehlerbehebung bei der RPC-Dienst-Verbindung“ auf Seite 98

Probleme oder Meldungen	Lösungen
`Unable to connect to Windows server...The network path was not found`	Netzwerk-Verbindungsfehler. Führen Sie die Tests in „Durchführen von Verbindungstests“ auf Seite 96 durch. Falls ein Test fehlschlägt, stellen Sie sicher, dass sich PlateSpin Forge und der Workload im selben Netzwerk befinden. Konfigurieren Sie das Netzwerk neu und versuchen Sie es erneut.

`“Discover Server Details {hostname}” Failed`
`Progress: 0%`
`Status: NotStarted`
	Dieser Fehler kann aus verschiedenen Gründen auftreten. Es gibt für jede Ursache eine eigene Lösung:
	◆ Bei Umgebungen, die einen lokalen Proxy mit Authentifizierung verwenden: Umgehen Sie den Proxy oder fügen Sie die richtigen Berechtigungen hinzu. Weitere Informationen hierzu finden Sie im KB-Beitrag 7920339 (http://www.novell.com/support/viewContent.do?externalId=7920339).
	◆ Wenn lokale oder Domänenrichtlinien die erforderlichen Berechtigungen einschränken, führen Sie die im KB-Artikel 7920862 (http://www.novell.com/support/viewContent.do?externalId=7920862) beschriebenen Schritte aus.

Workload-Ermittlungsfehler mit Fehlermeldung
`Could not find file output.xml`
oder
`Network path not found`
oder (beim Versuch, einen Windows-Cluster zu ermitteln)
`Inventory failed to discover.  Inventory result returned nothing.`
	Es gibt mehrere mögliche Gründe für den Fehler `Datei output.xml wurde nicht gefunden`:
	◆ Virenschutz-Software auf dem Ursprung könnte die Ermittlung beeinträchtigen. Deaktivieren Sie die Virenschutz-Software, um festzustellen, ob sie die Ursache für das Problem ist. Weitere Informationen hierzu finden Sie unter „Deaktivieren der Virenschutz-Software“ auf Seite 98.
	◆ Die Datei- und Drucker-Freigabe für Microsoft-Netzwerke ist möglicherweise nicht aktiviert. Aktivieren Sie die Freigabe in den Eigenschaften der Netzwerkschnittstellenkarte.
	◆ Die C$- und/oder Admin$-Freigaben auf dem Ursprung sind möglicherweise nicht zugänglich. Stellen Sie sicher, dass PlateSpin Forge auf diese Freigaben zugreifen kann. Weitere Informationen hierzu finden Sie unter „Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff“ auf Seite 98.
	◆ Ändern Sie den Wert für `ForceMachineDiscoveryUsingService` in der Datei `web.config` im Ordner `\Programme\PlateSpin Portability Suite Server\Web` in `true`.
	◆ Der Server- oder der Arbeitsstationsdienst läuft möglicherweise nicht. Wenn dies der Fall ist, aktivieren Sie den Dienst und stellen Sie den Startmodus auf `Automatisch` ein.
	◆ Der Remoteregistrierungsdienst von Windows ist deaktiviert. Starten Sie den Dienst und stellen Sie den Starttyp auf „Automatisch“ ein.

8.1.1 Durchführen von Verbindungstests

- „Netzwerk-Verbindungstest“ auf Seite 97
- „WMI-Verbindungstest“ auf Seite 97

* „Fehlerbehebung bei DCOM-Verbindungen“ auf Seite 97
* „Fehlerbehebung bei der RPC-Dienst-Verbindung“ auf Seite 98

Netzwerk-Verbindungstest

Führen Sie diesen Basistest der Netzwerkverbindung durch, um festzustellen, ob PlateSpin Forge mit dem Workload kommunizieren kann, den Sie zu schützen versuchen.

1 Wechseln Sie zu Ihrer Forge-VM.

Weitere Informationen hierzu finden Sie in „Herunterladen des VMware-Clientprogramms“ auf Seite 42.

2 Öffnen Sie ein Befehlszeilenfenster und senden Sie einen Ping-Befehl an Ihren Workload:

`ping` *`workload_ip`*

WMI-Verbindungstest

1 Wechseln Sie zu Ihrer Forge-VM.

Weitere Informationen hierzu finden Sie unter „Herunterladen des VMware-Clientprogramms“ auf Seite 42„Herunterladen des VMware-Clientprogramms“ auf Seite 42.

2 Klicken Sie auf *Start* > *Ausführen*, geben Sie `Wbemtest` ein und drücken Sie die `Eingabetaste`.

3 Klicken Sie auf *Verbinden*.

4 Geben Sie unter *Namespace* den Namen des Workloads ein, den Sie zu ermitteln versuchen, und hängen Sie `\root\cimv2` an den Namen an. Wenn der Hostname beispielsweise `win2k` lautet, geben Sie Folgendes ein:

`\\win2k\root\cimv2`

5 Geben Sie den entsprechenden Berechtigungsnachweis ein. Verwenden Sie hierzu entweder das Format `Hostname\LocalAdmin` oder `Domäne\DomainAdmin`.

6 Klicken Sie auf *Verbinden*, um die WMI-Verbindung zu testen.

Wenn eine Fehlermeldung zurückgegeben wird, kann keine WMI-Verbindung zwischen PlateSpin Forge und Ihrem Workload hergestellt werden.

Fehlerbehebung bei DCOM-Verbindungen

1 Melden Sie sich bei dem zu schützenden Workload an.

2 Klicken Sie auf *Start* > *Ausführen*.

3 Geben Sie `dcomcnfg` ein und drücken Sie die Eingabetaste.

4 Prüfen Sie die Verbindung:

* Auf einem Servercomputer mit Windows NT/2000 wird das Dialogfeld „DCOM-Konfiguration“ angezeigt. Klicken Sie auf die Registerkarte *Standardeigenschaften* und stellen Sie sicher, dass *DCOM (Distributed COM) auf diesem Computer aktivieren* ausgewählt ist.
* Bei Windows Server 2003 wird das Fenster „Komponentendienste“ angezeigt. Klicken Sie im Ordner *Computer* des Konsolenbaums im Verwaltungstool „Komponentendienste“ mit der rechten Maustaste auf den Computer, den Sie hinsichtlich der DCOM-Verbindung

prüfen möchten, und klicken Sie anschließend auf *Eigenschaften*. Klicken Sie auf die Registerkarte *Standardeigenschaften* und stellen Sie sicher, dass *DCOM (Distributed COM) auf diesem Computer aktivieren* ausgewählt ist.

5 Wenn DCOM nicht aktiviert ist, aktivieren Sie es und booten Sie entweder den Server neu oder starten Sie den Windows-Verwaltungsinstrumentation-Dienst neu. Versuchen Sie nun nochmals, den Workload hinzuzufügen.

Fehlerbehebung bei der RPC-Dienst-Verbindung

Es gibt drei potenzielle Blockaden beim RPC-Dienst:

- Der Windows-Dienst
- Eine Windows-Firewall
- Eine Hardware-Firewall

Stellen Sie für den Windows-Dienst sicher, dass der RPC-Dienst auf dem Workload ausgeführt wird. Führen Sie `services.msc` von einem Befehlszeilenfenster aus, um das Dienstefenster zu öffnen. Fügen Sie für eine Windows-Firewall eine RPC-Ausnahme hinzu. Bei Hardware-Firewalls können Sie folgende Strategien probieren:

- PlateSpin Forge und der Workload müssen sich auf derselben Seite der Firewall befinden
- Öffnen spezifischer Ports zwischen PlateSpin Forge und dem Workload (siehe „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“ auf Seite 23)

8.1.2 Deaktivieren der Virenschutz-Software

Virenschutz-Software kann gelegentlich einige der mit WMI und der Remoteregistrierung zusammenhängenden PlateSpin Forge-Funktionen blockieren. Um sicherzustellen, dass die Workload-Inventarisierung erfolgreich durchgeführt wird, muss gegebenenfalls zuerst der Virenschutzdienst auf einem Workload deaktiviert werden. Darüber hinaus kann Virenschutz-Software mitunter auch den Zugriff auf bestimmte Dateien sperren und nur den Zugriff auf bestimmte Prozesse oder Programmdateien zulassen. Dies kann mitunter die dateibasierte Datenreproduktion verhindern. Wenn Sie den Workload-Schutz konfigurieren, können Sie in diesem Fall die zu deaktivierenden Dienste auswählen, z. B. Dienste, die von Virenschutz-Software installiert und verwendet werden. Diese Dienste werden nur für die Dauer der Dateiübertragung deaktiviert. Sobald der Prozess abgeschlossen ist, werden sie wieder gestartet. Bei einer Datenreproduktion auf Blockebene ist dies nicht erforderlich.

8.1.3 Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff

Für den erfolgreichen Schutz eines Workloads muss PlateSpin Forge den OFX-Controller und, falls eine Reproduktion auf Blockebene erforderlich ist, eine dedizierte blockbasierte Komponente erfolgreich bereitstellen und installieren. Bei der Bereitstellung dieser Komponenten auf einem Workload sowie während des Hinzufügens eines Workloads verwendet PlateSpin Forge die administrativen Freigaben des Workloads. PlateSpin Forge benötigt Administratorzugriff auf die Freigaben und verwendet dazu ein lokales Administratorkonto oder ein Domänen-Administratorkonto.

So stellen Sie sicher, dass die administrativen Freigaben aktiviert sind:

1. Klicken Sie mit der rechten Maustaste auf *Arbeitsplatz* auf dem Desktop und wählen Sie *Verwalten*.
2. Erweitern Sie *System* > *Freigegebene Ordner* > *Freigaben*.
3. Im Verzeichnis `Freigegebene Ordner` müssten neben anderen die Freigaben C$ und Admin$ vorhanden sein.

Nachdem Sie sich vergewissert haben, dass die Freigaben aktiviert sind, stellen Sie sicher, dass sie von der Forge-VM aus zugänglich sind:

1. Wechseln Sie zu Ihrer Forge-VM.

   Weitere Informationen hierzu finden Sie in „Herunterladen des VMware-Clientprogramms“ auf Seite 42.
2. Klicken Sie auf *Start* > *Ausführen*, geben Sie `\\<Server-Host>\C$` ein und klicken Sie anschließend auf *OK*.
3. Verwenden Sie bei Aufforderung denselben Berechtigungsnachweis wie für das Hinzufügen des Workloads zum PlateSpin Forge-Workload-Inventar.

   Das Verzeichnis wird geöffnet und Sie sollten in der Lage sein, darin zu navigieren und seinen Inhalt zu ändern.
4. Wiederholen Sie diesen Vorgang für alle Freigaben außer der IPC$-Freigabe.

   Windows verwendet die IPC$-Freigabe für die Berechtigungsnachweisvalidierung und Authentifizierung. Sie ist nicht einem Ordner oder einer Datei im Workload zugeordnet, der Test schlägt daher immer fehl. Die Freigabe sollte aber weiterhin sichtbar sein.

PlateSpin Forge ändert den vorhandenen Inhalt des Volumes nicht. Es erstellt jedoch ein eigenes Verzeichnis, für das es Zugriff und Berechtigungen benötigt.

8.2 Fehlerbehebung bei der Workload-Inventarisierung (Linux)

Probleme oder Meldungen	Lösungen
`Es konnte weder eine Verbindung zum SSH-Server, der auf <IP-Adresse> läuft, noch zu den VMware Virtual Infrastructure-Webdiensten unter <IP-Adresse>/sdk hergestellt werden`	Diese Meldung wird aufgrund mehrerer möglicher Ursachen ausgegeben: ◆ Der Workload ist nicht erreichbar. ◆ Auf dem Workload wird SSH nicht ausgeführt. ◆ Die Firewall ist aktiv und die erforderlichen Ports wurden nicht geöffnet. ◆ Das spezifische Betriebssystem des Workloads wird nicht unterstützt Informationen zu Netzwerk- und Zugriffsanforderungen für einen Workload finden Sie unter „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“ auf Seite 23.

Probleme oder Meldungen	Lösungen
`Access denied`	Dieses Authentifizierungsproblem weist auf einen ungültigen Benutzernamen oder ein ungültiges Passwort hin. Weitere Informationen über den richtigen Berechtigungsnachweis für den Workload-Zugriff finden Sie unter „Richtlinien für Workload-Berechtigungsnachweise“ auf Seite 83.

8.3 Beheben von Problemen während der Ausführung des Befehls „Reproduktion vorbereiten“ (Windows)

Probleme oder Meldungen	Lösungen
Authentifizierungsfehler beim Überprüfen der Controller-Verbindung während der Einrichtung des Controllers auf dem Ursprung.	Das für das Hinzufügen eines Workloads verwendete Konto muss von dieser Richtlinie zugelassen sein. Weitere Informationen hierzu finden Sie unter „Gruppenrichtlinie und Benutzerrechte“ auf Seite 100.
Es konnte nicht festgestellt werden, ob .NET Framework installiert ist (mit Ausnahme `Die vertrauenswürdige Beziehung zwischen dieser Arbeitsstation und der primären Domäne ist fehlgeschlagen`).	Überprüfen Sie, ob der Remoteregistrierungsdienst auf dem Ursprung aktiviert ist und ausgeführt wird. Siehe auch „Fehlerbehebung bei der Workload-Inventarisierung (Windows)“ auf Seite 95.

8.3.1 Gruppenrichtlinie und Benutzerrechte

Sie können die Richtlinie sofort mithilfe von `gpudate /force` (bei Windows 2003/XP) oder `secedit /refreshpolicy machine_policy /enforce` (bei Windows 2000) aktualisieren. Aufgrund der Art und Weise, wie PlateSpin Forge mit dem Betriebssystem des Ursprungs-Workloads interagiert, muss das zum Hinzufügen des Workloads verwendete Administratorkonto über bestimmte Benutzerrechte auf dem Ursprungscomputer verfügen. In den meisten Fällen sind diese Einstellungen Standardwerte der Gruppenrichtlinie. Wenn die Umgebung jedoch gesperrt wurde, wurden folgende Benutzerrechte-Zuweisungen möglicherweise entfernt:

- Traverse Checking umgehen
- Token auf Prozessebene ersetzen
- Als Teil des Betriebssystems agieren

Um zu überprüfen, ob diese Gruppenrichtlinien-Einstellungen festgelegt wurden, können Sie `gpresult /v` von der Befehlszeile auf dem Ursprungscomputer oder alternativ `RSOP.msc` ausführen. Wenn die Richtlinie nicht festgelegt oder wenn sie deaktiviert wurde, kann sie über die lokale Sicherheitsrichtlinie des Computers oder über eine der für den Computer geltenden Domänengruppenrichtlinien aktiviert werden.

8.4 Fehlerbehebung bei der Workload-Reproduktion

Probleme oder Meldungen	Lösungen
Workload-Problem erfordert Benutzereingriff Behebbarer Fehler bei der Reproduktion während des Vorgangs *Erstellen eines Snapshots der virtuellen Maschine planen* oder *Planen des Zurücksetzens der virtuellen Maschine auf Snapshot vor dem Start*.	Dieses Problem tritt auf, wenn der Server ausgelastet ist und der Vorgang länger als erwartet dauert. Die Lösung besteht darin, bis zum Abschluss der Reproduktion zu warten.
Bei allen Workloads treten behebbare Fehler auf, da kein Speicherplatz mehr vorhanden ist.	Überprüfen Sie den freien Speicherplatz. Wenn mehr Platz erforderlich ist, entfernen Sie einen Workload.
Langsame Netzwerkgeschwindigkeiten unter 1 MB.	Stellen Sie sicher, dass die Duplex-Einstellung der Netzwerkschnittstellenkarte des Ursprungscomputers aktiviert ist und dass der Switch, mit dem sie verbunden ist, eine entsprechende Einstellung hat. Wenn der Switch auf automatisch gesetzt ist, kann der Ursprung nicht auf 100 MB eingestellt werden.
Langsame Netzwerkgeschwindigkeiten über 1 MB.	Messen Sie die Latenz, indem Sie folgenden Befehl vom Ursprungs-Workload aus ausführen: `ping` *`ip`* `–t` (ersetzen Sie *ip* durch die IP-Adresse Ihrer Forge-VM). Lassen Sie den Befehl für 50 Iterationen ausführen. Der Durchschnitt gibt dann die Latenz an. Siehe auch „Parameter für die Optimierung von Übertragungen in WAN-Verbindungen“ auf Seite 30.

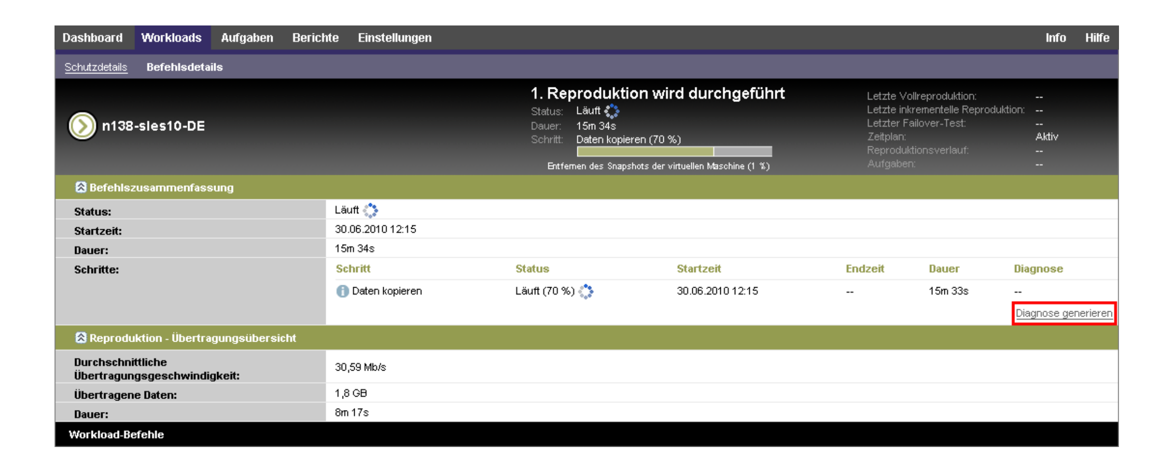
`The file transfer cannot begin - port 3725 is already in use`
 	
oder
 	
`3725 unable to connect`
	Stellen Sie sicher, dass der Port offen ist und überwacht:
	
	Führen Sie `netstat -ano` auf dem Workload aus.
	
	Überprüfen Sie die Firewall.
	
	Wiederholen Sie die Reproduktion.

Probleme oder Meldungen	Lösungen
`Controller connection not established` Die Reproduktion schlägt beim Schritt *Kontrolle über die virtuelle Maschine übernehmen* fehl.	Dieser Fehler tritt auf, wenn die Reproduktionsnetzwerkinformationen ungültig sind. Entweder ist der DHCP-Server nicht verfügbar oder das virtuelle Reproduktionsnetzwerk kann keine Verbindung zur Forge-VM herstellen. Ändern Sie die Reproduktions-IP in eine statische IP oder aktivieren Sie den DHCP-Server. Stellen Sie sicher, dass das für die Reproduktion ausgewählte virtuelle Netzwerk eine Verbindung zur Forge-VM herstellen kann.
Der Reproduktionsauftrag startet nicht (hängt bei 0 %)	Dieser Fehler kann aus unterschiedlichen Gründen auftreten. Es gibt für jede Ursache eine eigene Lösung: ◆ Bei Umgebungen, die einen lokalen Proxy mit Authentifizierung verwenden: Umgehen Sie den Proxy oder fügen Sie die richtigen Berechtigungen hinzu, um dieses Problem zu beheben. Weitere Informationen hierzu finden Sie im KB-Beitrag 20339 (http://www.novell.com/support/viewContent.do?externalId=7920339). ◆ Wenn lokale oder Domänenrichtlinien die erforderlichen Berechtigungen einschränken, führen Sie die im KB-Artikel 7920862 (http://www.novell.com/support/viewContent.do?externalId=7920862) beschriebenen Schritte aus. Dieses Problem tritt häufig auf, wenn die Forge-VM mit einer Domäne verbunden ist und die Domänenrichtlinien mit Einschränkungen angewendet werden. Weitere Informationen hierzu finden Sie unter „Gruppenrichtlinie und Benutzerrechte“ auf Seite 100.

8.5 Generieren und Anzeigen von Diagnoseberichten

Nachdem Sie im PlateSpin Forge Web-Client einen Befehl ausgeführt haben, können Sie detaillierte Diagnoseberichte über die Details des Befehls generieren.

1 Klicken Sie auf *Befehlsdetails* und dann auf *Diagnose generieren*.



Nach kurzer Zeit wird die Seite aktualisiert und zeigt den Link *Ansicht* oberhalb des Links *Diagnose generieren* an.

2 Klicken Sie auf *Anzeigen*.

Es wird eine neue Seite mit umfassenden Diagnoseinformationen zum aktuellen Befehl geöffnet.

3 Speichern Sie die Diagnoseseite und halten Sie sie bereit, falls Sie den technischen Support kontaktieren müssen.

8.6 Workload-Bereinigung nach dem Schutz

Befolgen Sie dieses Schritte, um Ihren Ursprungs-Workload von allen PlateSpin-Software-Komponenten zu bereinigen, falls dies erforderlich ist, wie z. B. nach einem erfolglosen oder problematischen Schutz.

8.6.1 Bereinigen von Windows-Workloads

Komponente	Entfernungsanweisung
Blockbasierte PlateSpin-Übertragungskomponente	Weitere Informationen hierzu finden Sie im KB-Artikel 7005616 (http://www.novell.com/support/viewContent.do?externalId=7005616).
Blockbasierte Übertragungskomponente eines Drittanbieters (eingestellt)	1. Windows Software-Applet verwenden (`appwiz.cpl` ausführen) und die Komponenten entfernen. Abhängig vom Ursprung haben Sie eine der folgenden Versionen: ◆ SteelEye Data Replication for Windows v6 Update2 ◆ SteelEye DataKeeper For Windows v7 2. Booten Sie den Computer neu.
Dateibasierte Übertragungskomponente	Auf Root-Ebene für jedes geschützte Volume alle Dateien namens `PlateSpinCatalog*.dat` entfernen.

Komponente	Entfernungsanweisung
Workload-Inventarisierungs-software	Im `Windows`-Verzeichnis des Workloads: ◆ Alle Dateien namens `machinediscovery*` entfernen. ◆ Unterverzeichnis `platespin` entfernen.
Controller-Software	1. Eine Eingabeaufforderung öffnen und das aktuelle Verzeichnis ändern in: ◆ `\Programme\platespin*` (32-Bit-Systeme) ◆ `\Programme (x86)\platespin` (64-Bit-Systeme) 2. Führen Sie den folgenden Befehl aus: `ofxcontroller.exe /uninstall` 3. Verzeichnis `platespin*` entfernen.

8.6.2 Bereinigen von Linux-Workloads

Komponente	Entfernungsanweisung
Controller-Software	◆ Diese Prozesse stoppen: ◆ `pkill -9 ofxcontrollerd` ◆ `pkill -9 ofxjobexec` ◆ Das OFX-Controller-rpm-Package entfernen: `rpm -e ofxcontrollerd` ◆ Im Dateisystem des Ursprungs-Workloads das Verzeichnis `/usr/lib/ofx` mit Inhalt entfernen.

Software für den Datentransfer auf Blockebene	1. Prüfen Sie, ob der Treiber aktiv ist:
	`lsmod | grep blkwatch`
	Wenn der Treiber immer noch im Arbeitsspeicher geladen ist, sollte das Ergebnis eine Zeile wie die folgende enthalten:
	`blkwatch_7616  70924  0`
	2. (Bedingt) Wenn der Treiber noch geladen ist, entfernen Sie ihn aus dem Arbeitsspeicher:
	`rmmod blkwatch_7616`
	3. Entfernen Sie den Treiber aus der Boot-Sequenz:
	`blkconfig -u`
	4. Entfernen Sie die Treiberdateien, indem Sie das folgende Verzeichnis mitsamt Inhalt löschen:
	`/lib/modules/`*`[Kernel_Version]`*`/Platespin`
	5. Löschen Sie die folgende Datei:
	`/etc/blkwatch.conf`

Komponente	Entfernungsanweisung
LVM-Snapshots	1. In der Ansicht „Aufträge“ einen Auftragsbericht für den fehlgeschlagenen Auftrag generieren und den Namen des Snapshot notieren. 2. Das Snapshot-Gerät unter Verwendung des folgenden Befehls entfernen: `lvremove` *Snapshot-Name*
Bitmap-Dateien	Bei jedem geschützten Volume im Volume-Stamm die entsprechende `.blocks_bitmap`-Datei entfernen.
Werkzeuge	Im Ursprungs-Workload unter `/sbin` folgende Dateien entfernen: ◆ `bmaputil` ◆ `blkconfig`

8.6.3 Entfernen von Workloads

In einigen Situationen müssen Sie unter Umständen einen Workload vom PlateSpin Forge-Inventar entfernen und später wieder hinzufügen.

1. Wählen Sie auf der Seite „Workloads“ den zu entfernenden Workload aus und klicken Sie anschließend auf *Workload entfernen*.

   (Bedingt) Bei Windows-Workloads, die zuvor durch eine Reproduktion auf Blockebene geschützt wurden, fordert der PlateSpin Forge Web-Client Sie auf anzugeben, ob Sie auch die blockbasierten Komponenten entfernen möchten. Folgenden Optionen stehen zur Auswahl:

   - **Komponenten nicht entfernen:** Die Komponenten werden nicht entfernt.
   - **Komponenten entfernen, Workload aber nicht neu starten:** Die Komponenten werden entfernt. Es ist jedoch ein Neustart des Workloads erforderlich, um den Deinstallationsprozess abzuschließen.
   - **Komponenten entfernen und Workload neu starten:** Die Komponenten werden entfernt und der Workload wird automatisch neu gestartet. Stellen Sie sicher, dass Sie diesen Vorgang während der geplanten Ausfallzeit durchführen.

2. Klicken Sie auf auf der Seite „Befehlsbestätigung“ auf *Bestätigen*, um den Befehl auszuführen.

   Warten Sie, bis der Vorgang abgeschlossen ist.

Glossar

Appliance-Host

Weitere Informationen hierzu finden Sie unter Container.

Container

Der VM-Host, der den Wiederherstellungs-Workload (die bootfähige virtuelle Reproduktion eines geschützten Workloads) enthält.

Ereignis

Eine PlateSpin Forge Server-Nachricht, die Informationen über wichtige Schritte während des gesamten Workload-Schutz-Lebenszyklus enthält.

Failback

Die Wiederherstellung der Geschäftsfunktion eines fehlgeschlagenen Workloads in seiner ursprünglichen Umgebung, wenn die Geschäftsfunktion eines temporären Wiederherstellungs-Workloads in PlateSpin Forge nicht mehr benötigt wird.

Failover

Die Übernahme der Geschäftsfunktion eines fehlgeschlagenen Workloads von einem Wiederherstellungs-Workload innerhalb eines PlateSpin Forge-VM-Containers.

inkrementell

1. (Substantiv) Eine einzelne geplante oder manuelle Übertragung von Unterschieden zwischen einem geschützten Workload und dessen Reproduktion (dem Wiederherstellungs-Workload).

2. (Adjektiv) Beschreibt den Umfang der *Reproduktion (1)*, in dem die anfängliche Reproduktion eines Workloads differentiell erstellt wird (auf der Basis von Unterschieden zwischen dem Workload und seinem vorbereiteten Gegenstück.

Management-VM

Die virtuelle Management-Maschine, die die PlateSpin Forge-Software enthält.

Vorbereiten auf Failover

Ein PlateSpin Forge-Vorgang, der den Wiederherstellungs-Workload in Vorbereitung eines vollständigen Failover-Vorgangs bootet.

Schutzebene

Eine benutzerdefinierbare Sammlung an Workload-Schutz-Parametern, die die Häufigkeit von Reproduktionen definiert sowie die Kriterien festlegt, anhand derer das System einen Workload als fehlgeschlagen erachtet.

Wiederherstellungspunkt

Ein zu einem bestimmten Zeitpunkt erstellter Snapshot, der es ermöglicht, einen reproduzierten Workload in einen früheren Zustand zurückzuversetzen.

Angestrebter Wiederherstellungszeitpunkt (RPO)

In Zeit gemessener tolerierbarer Datenverlust, der durch ein konfigurierbares Intervall zwischen inkrementellen Reproduktionen eines geschützten Workloads definiert wird.

Angestrebte Wiederherstellungszeit (RTO)

Ein Wert für die tolerierbare Ausfallzeit eines Workloads, definiert durch die Zeit, die für einen Failover-Vorgang erforderlich ist.

Wiederherstellungs-Workload

Die bootfähige virtuelle Reproduktion eines geschützten Workloads.

Reproduktion

1. Die Erstellung einer anfänglichen Basiskopie eines Workloads (*anfängliche Reproduktion*).

2. Jegliche Übertragung geänderter Daten von einem geschützten Workload auf seine Reproduktion im Container.

Reproduktionszeitplan

Der zur Steuerung der Häufigkeit und des Umfangs von Reproduktionen eingerichtete Zeitplan.

Erneut schützen

Ein PlateSpin Forge-Befehl, der einen Schutzvertrag für einen Workload nach Failover- und Failback-Vorgängen wiederherstellt.

Ursprung

Ein Workload oder dessen Infrastruktur, der bzw. die der Ausgangspunkt für einen PlateSpin Forge-Vorgang ist. Beispielsweise ist der Ursprung beim anfänglichen Schutz eines Workloads der Produktions-Workload. Bei einem Failback-Vorgang ist es der Wiederherstellungs-Workload im Container.

Siehe auch Ziel.

Ziel

Ein Workload oder dessen Infrastruktur, der bzw. die das Ergebnis eines PlateSpin Forge-Befehls ist. Beispielsweise ist das Ziel beim anfänglichen Schutz eines Workloads der Wiederherstellungs-Workload im Container. In einem Failback-Vorgang ist es entweder die Original-Infrastruktur des Produktions-Workloads oder ein unterstützter Container, der von PlateSpin Forge inventarisiert wurde.

Siehe auch Ursprung.

Failover testen

Ein PlateSpin Forge-Vorgang, bei dem ein Wiederherstellungs-Workload in einer isolierten Netzwerkumgebung gebootet wird, um die Funktionalität des Failovers zu testen und um die Integrität des Wiederherstellungs-Workloads zu überprüfen.

Angestrebte Testzeit (TTO)

Ein Maß dafür, wie einfach sich ein Wiederherstellungsplan für den Katastrophenfall testen lässt. Es entspricht weitgehend der RTO, umfasst jedoch auch die Zeit, die ein Benutzer zum Testen des Wiederherstellungs-Workloads benötigt.

Workload

Das Basis-Schutzobjekt in einer Datenablage. Ein Betriebssystem einschließlich dessen Middleware und Daten, das von der zugrunde liegenden physischen oder virtuellen Infrastruktur abgekoppelt ist.